FORTINET®

FAST. SECURE. GLOBAL.

FortiSandbox Workshop

© Copyright Fortinet Inc. All rights reserved.

FortiSandbox Positioning

FORTINET

General Threat Environment

- Gartner says all organizations should assume they are in a state of continuous compromise
- 2014/2015 were full of data breaches
- Many breaches remain undiscovered for months or a year
- Verizon Data Breach Reports

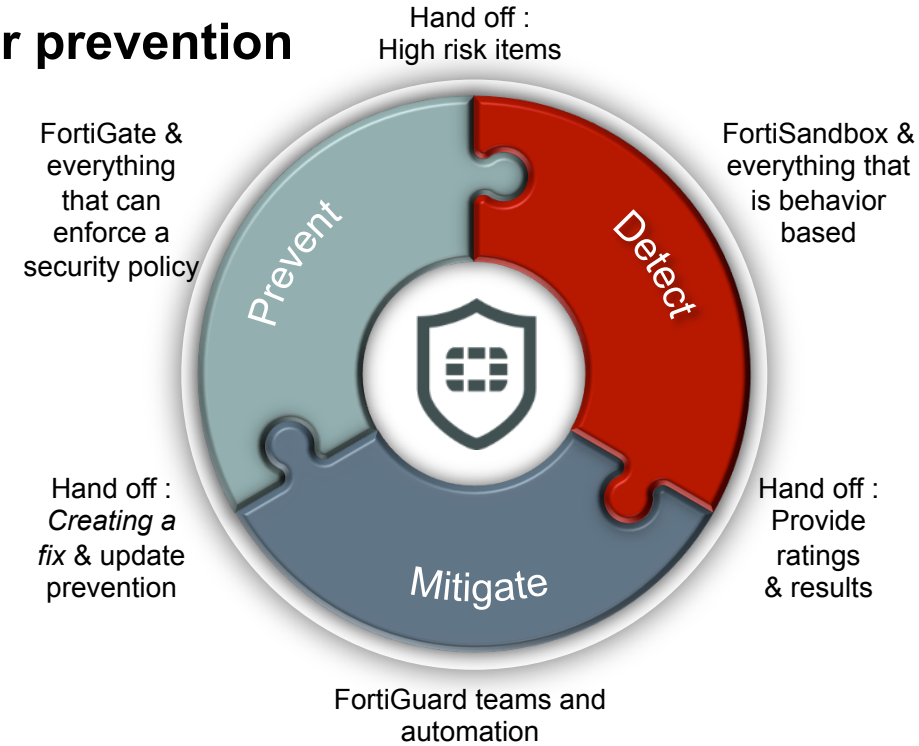
Advanced Threat Protection System

Turn the unknown into the known for prevention

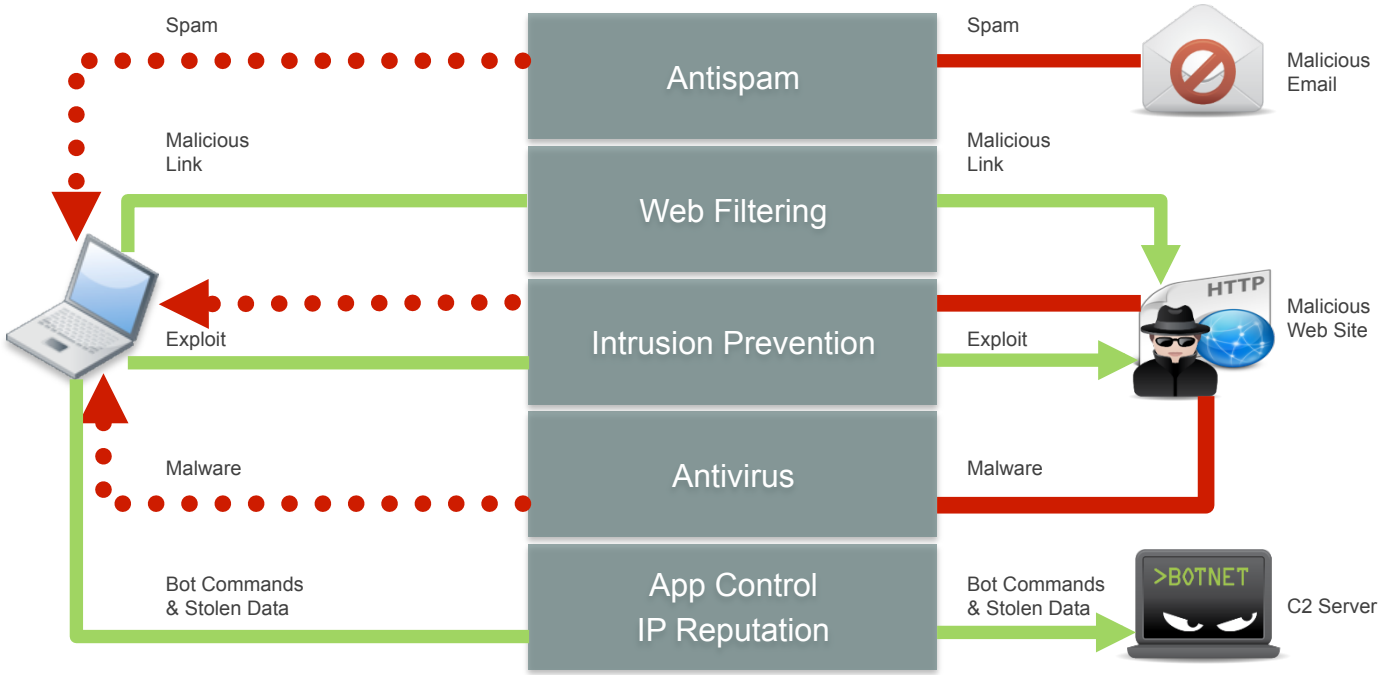
Known Threats
- Reduce Attack Surface
- Inspect & Block Known Threats

Unknown Threats
- Identify Unknown Threats
- Assess Behavior & Identify Trends

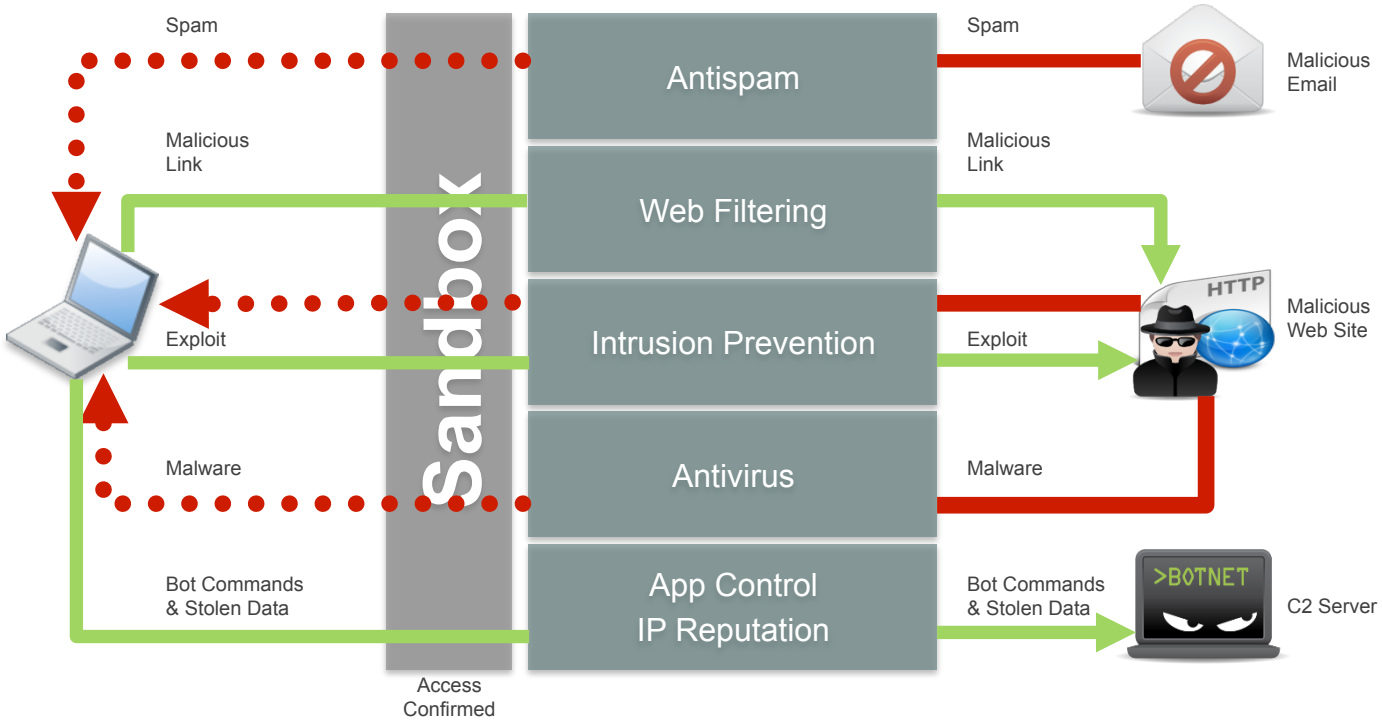
Response
- Identify scope
- Mitigate impact



Breaking the Kill Chain of Advanced Attacks



Breaking the Kill Chain of Advanced Attacks



NSS Labs BDS 2015 - FortiSandbox

Product				Detection Rate[1]	NSS-Tested Throughput
Fortinet FortiSandbox-1000D v1.43 Build 0120				97.3%	1,000 Mbps
HTTP Malware	**Email Malware**	**SMB Malware**	**Drive-by Exploits**	**Social Exploits**	**Evasions**
98.7%	99.1%	100.0%	94.5%	96.3%	58.2%

Figure 1 – Overall Test Results

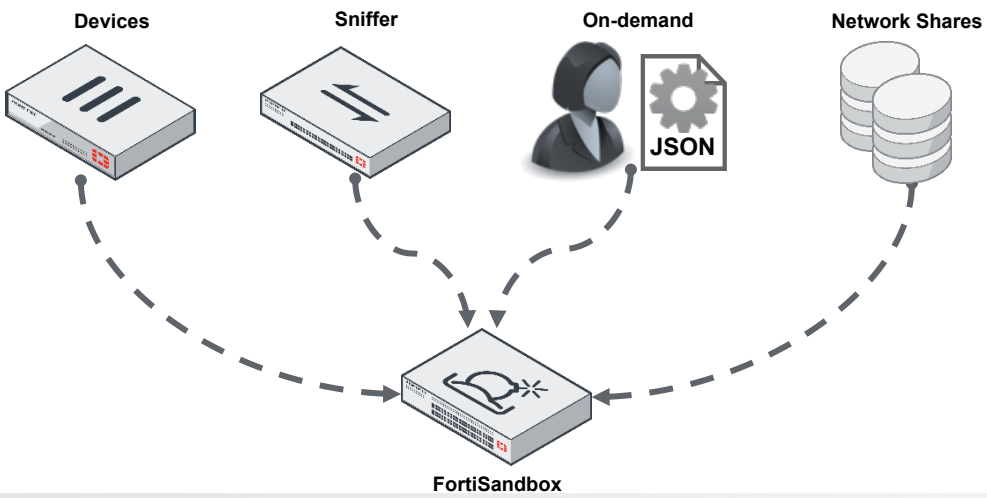
What is FortiSandbox?

An ATP Appliance

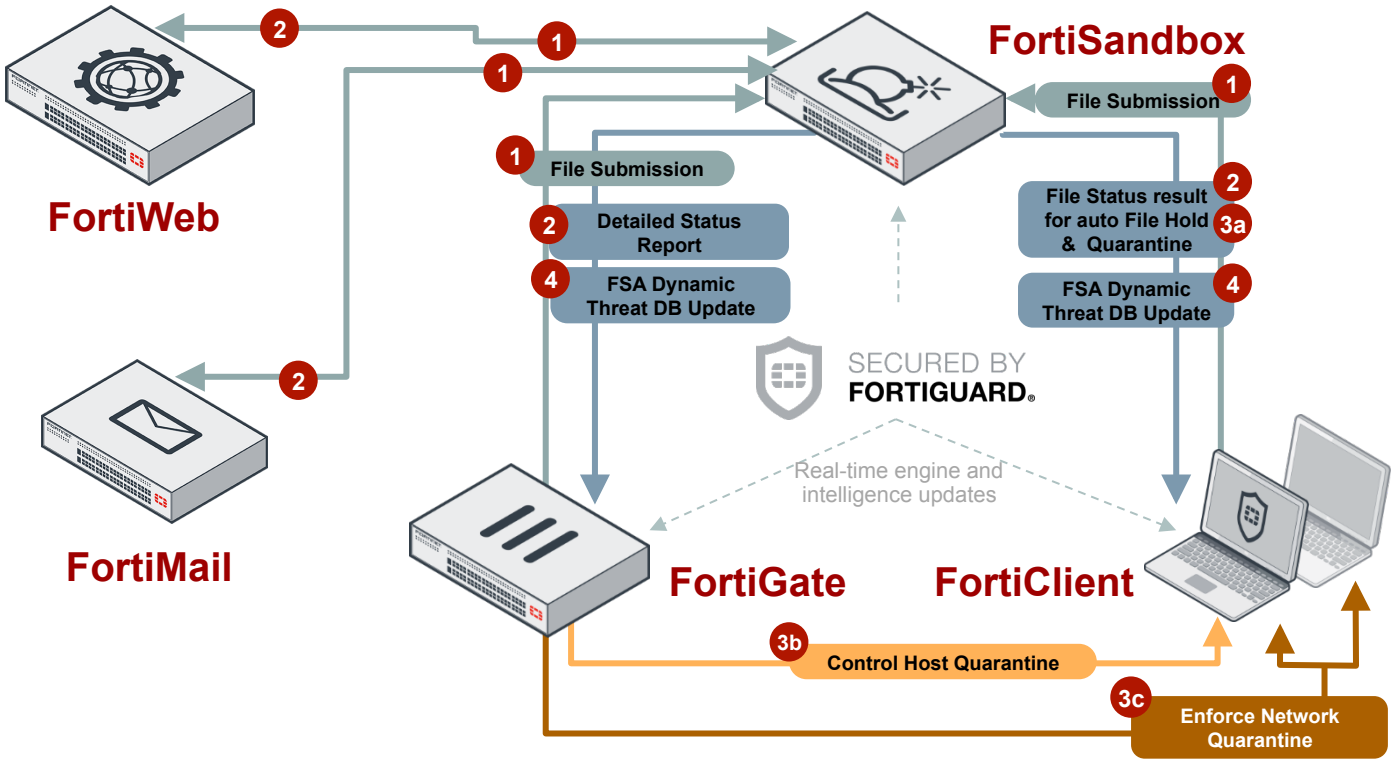
- Flexible Input Modes
  - » Devices, Sniffer, On-demand, Network Share
- Flexible Deployment Modes
  - » Standalone
  - » Integrated or Distributed
- Dual level Sandboxing
  - » Pre-filtering with AV + code emulation
  - » Sandbox VM
- FortiGuard Services
  - » File Query
  - » File Submission
  - » IP Reputation
  - » URL Rating
- Rating Engine
  - » Static analysis tools
  - » FortiGuard Intelligence
- Monitoring & Reporting

Supported Input Methods

- Devices
  - » Files submitted from a Fortinet product
- Sniffer
  - » Files extraction from monitored traffic
- On-demand
  - » Manual submission
  - » From WebUI
  - » From JSON-RPC API
- Network Shares
  - » Inspect Files on a CIFS/NFS share



Devices Input Method



Query

1. File submission for Analysis
2. Respective analysis results are returned

Remediation

3a. Auto File Quarantine on Host with option to hold file until result

3b. Manual Host Quarantine by Admin

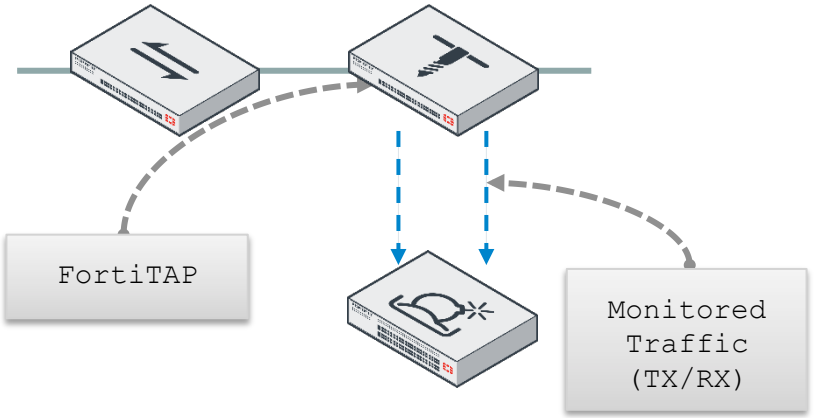
3c. Manual Source IP Quarantine using Firewall

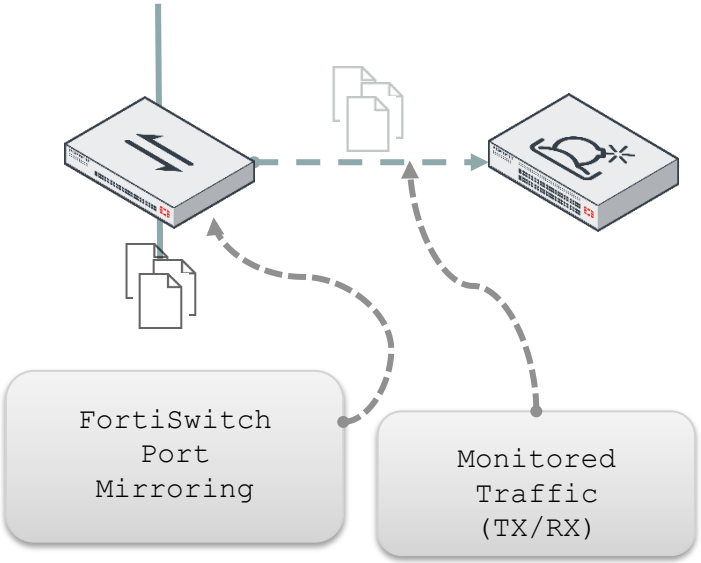
Protection

4. Proactive dynamic Threat DB update to gateway and host

Sniffer Input Method

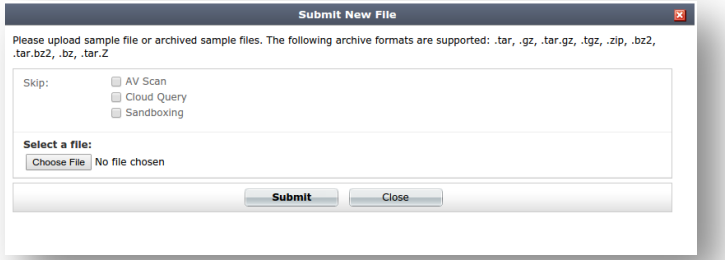
- Monitor the network traffic through two possible connections methods:
  - » Mirroring/monitoring or SPAN ports
  - » TAP device





On-Demand Input Method

- Administrator uses the web-based Manager or JSON-RPC API to upload files he wants to submit for inspection.
- Security Feature Exemption
  - » AV Scan
  - » Cloud File Query
  - » Sandboxing
- Tracking of the inspection through the On-Demand page

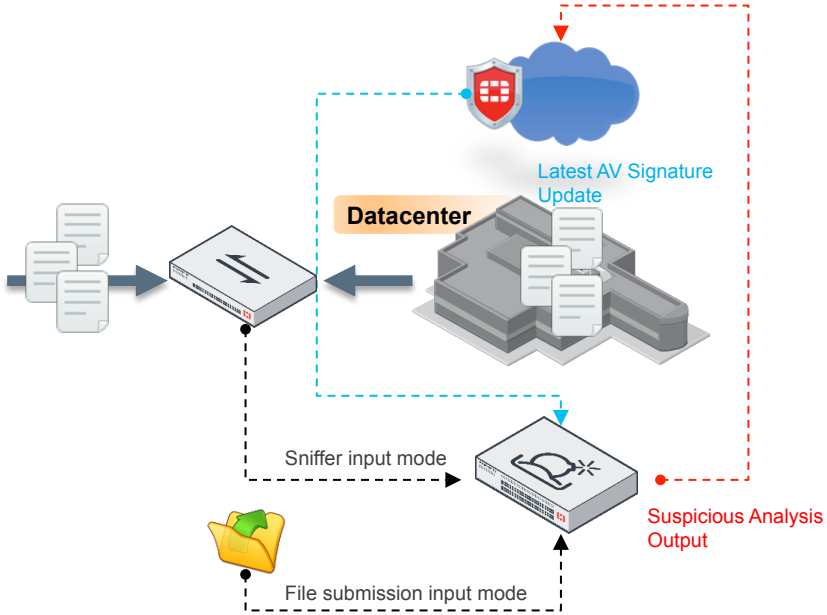



```
$ fsa.py -verbose -host 192.168.193.237 -user
admin -password admin -action submit-file -
file sample.exe -skip-steps 1,2
```

Network Shares

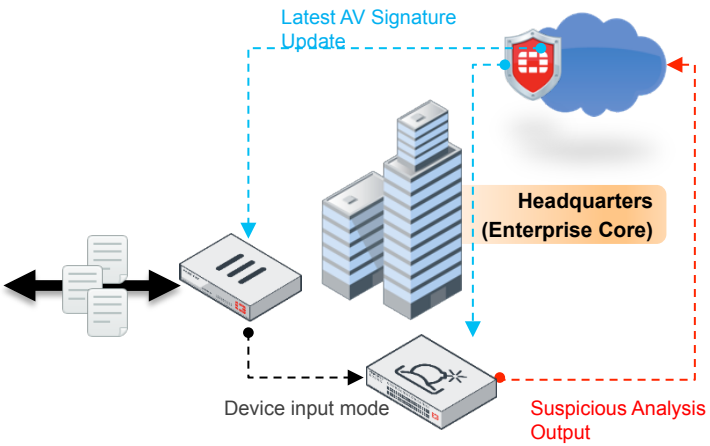
- CIFS or NFS
- On-Demand or Scheduled Inspection
- Quarantine Support
- Threat Intelligence Sharing

Deployment Mode: Standalone



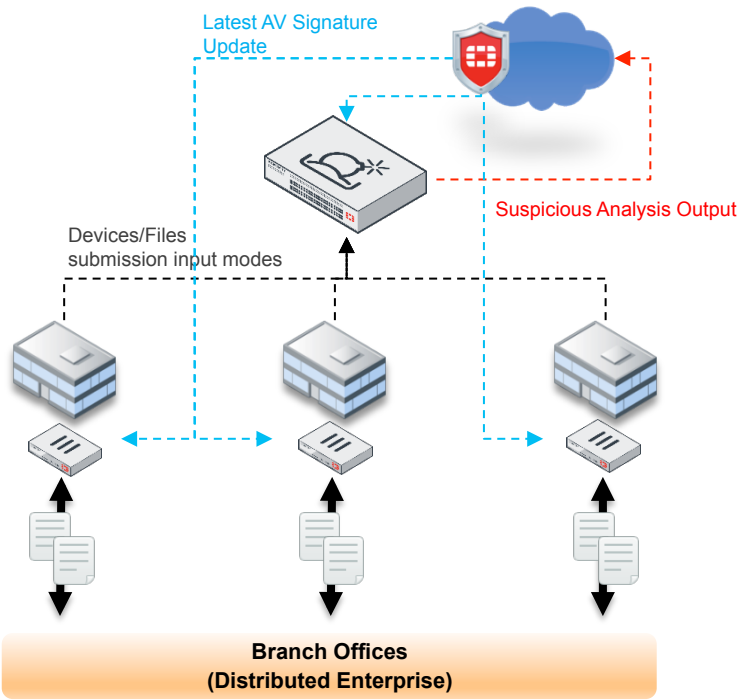
- Most suitable for adding **Threats Protection System** for **various vendors**
- Supported input methods
  - » Sniffer
  - » On-Demand

Deployment Mode: Integrated



- Seamless integration with Fortinet products
- Supported input methods
  - » Devices
  - » On-demand
- Support encrypted applications and protocols

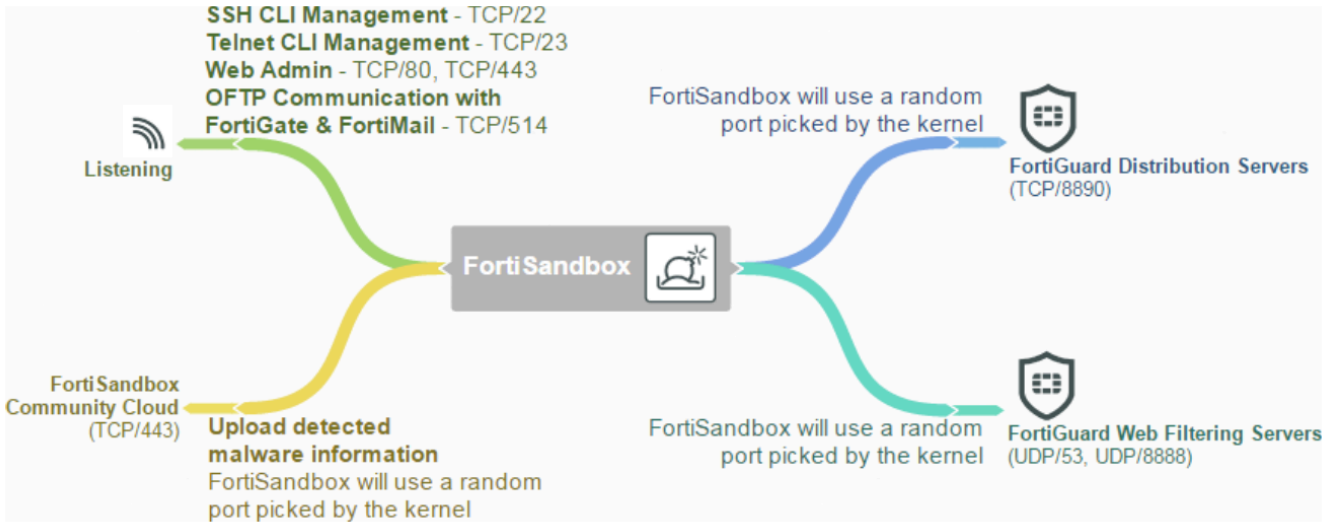
Deployment Mode: Distributed Integrated



- Distributed environments
- FortiGate deployed in remote branch offices
- Submit files to a centrally-located FortiSandbox
- Supported input methods
  - » Devices
  - » On-Demand

Communication Channels

- Incoming and Outgoing Ports



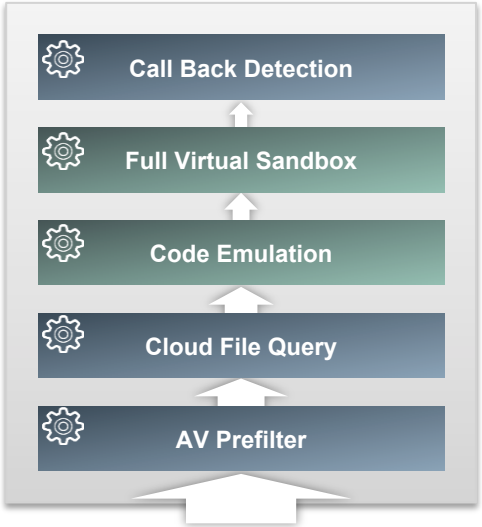
FortiSandbox Processing

Layered Security Features

FORTINET

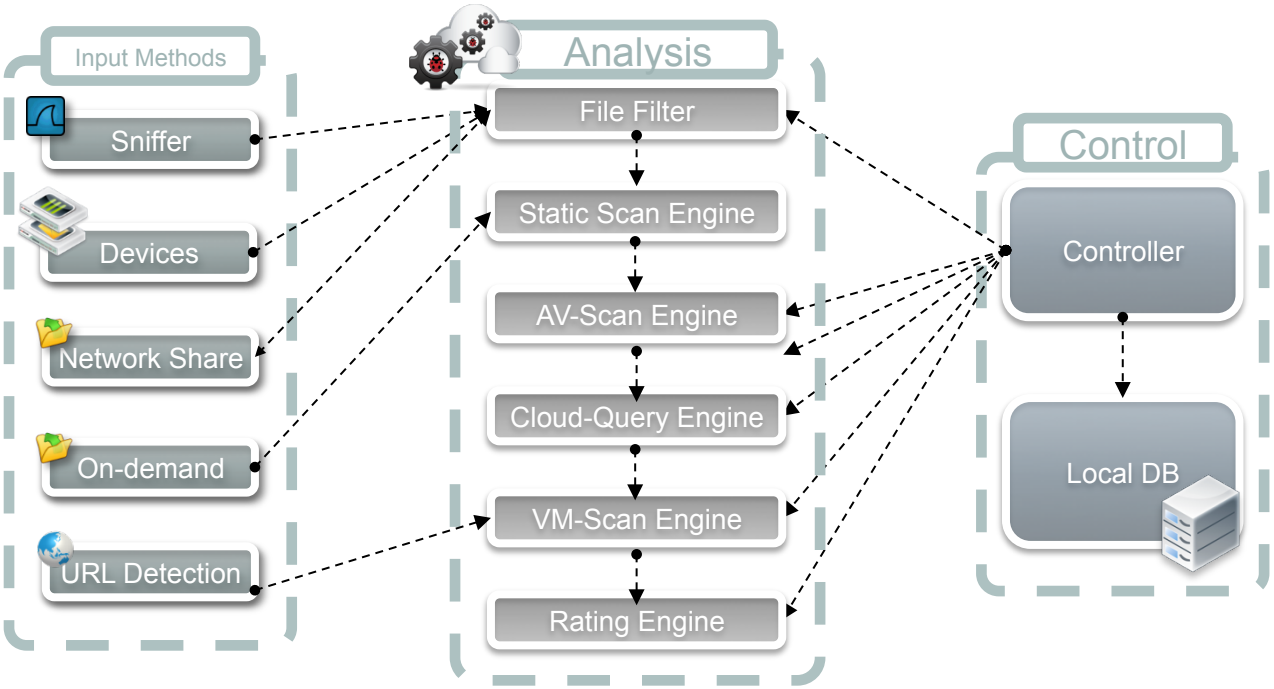
Process Overview

- Multi-tiered file processing optimizes resource usage to improve security, capacity and performance



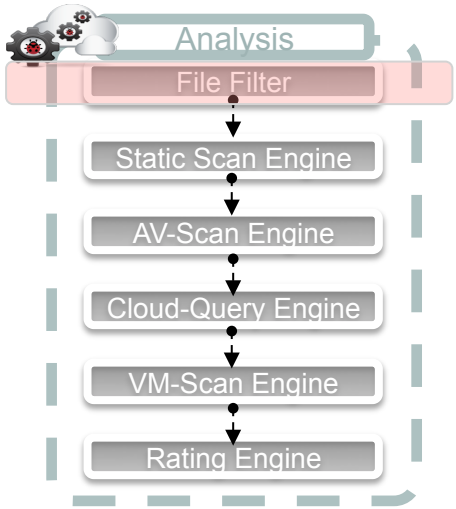
- Identify the ultimate aim, call back & exfiltration
- Mitigate w/ analytics & FortiGuard updates
- Examine real-time, full lifecycle activity in the sandbox to get the threat to expose itself
- Quickly simulate intended activity – Fortinet patented CPRL
- OS independent & immune to evasion – high catch rate
- Check community intelligence & file reputation
- Apply top-rated anti-malware engine

Processing In Detail



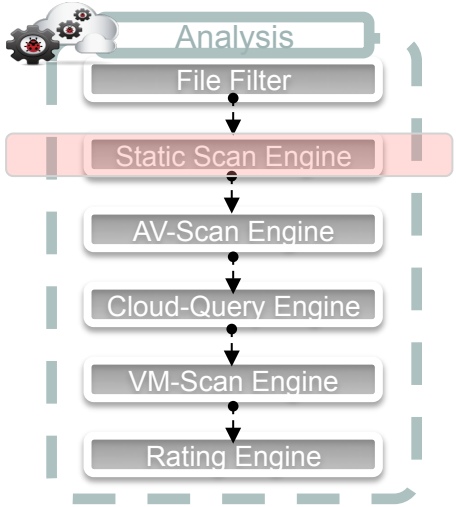
File Filter

- Step to provide initial filtration capability
- Determines if file is capable of instantiation or otherwise has ability to perform action within a computer instance
- Checks for “magic number” of file and queues based on output
- EXE/DLL, PDF, Office, SWF, JAR, and archive files are queued for full instantiation
- Other file types are sent to AV scanner and dropped



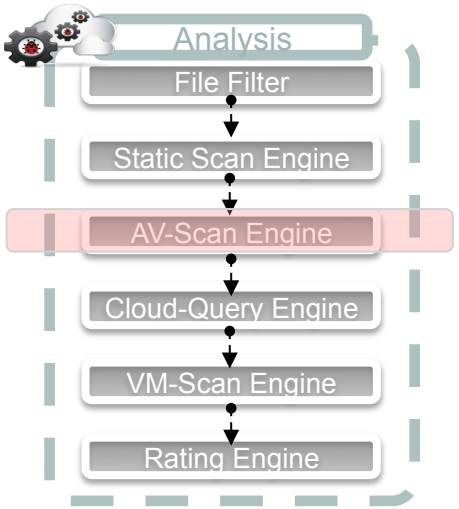
Static Scan

- Static Scan
  - » Calculate checksum
  - » Scan JS and PDF files
    - Execution based on YARA engine
    - Upload custom YARA rules
    - http://code.google.com/p/yara-project
    - http://plusvic.github.io/yara/
    - https://github.com/YaraExchange



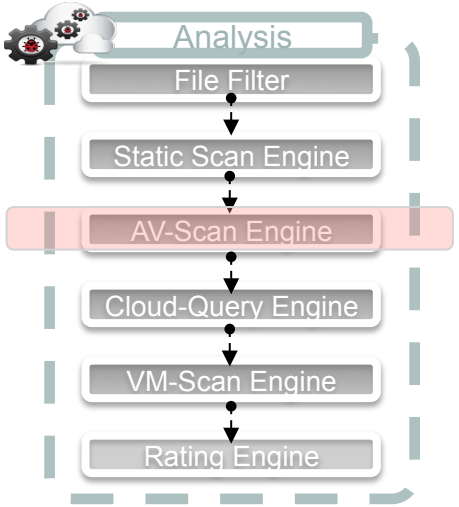
AV Scan Engine

- AV Scan
  - » Same AV scanner used in FGT models (Active & Extreme DB)
  - » Standard AV DB updates through FDN
  - » Any detected KNOWN virus will be rated as **Malicious** on FSA
- The Fortinet's antivirus engine decodes and tracks behaviors of polymorphic, encrypted and packed malware in realtime.
- Commonly used by authors of APTs, these evasion techniques enable advanced malware to bypass other detection engines
- How to detect them efficiently? CPRL and Code Emulation



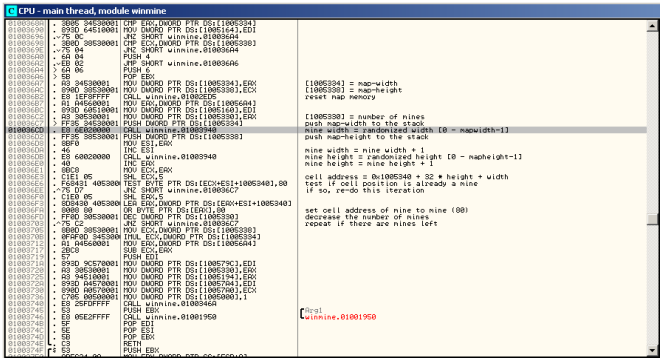
AV Scan Engine - CPRL

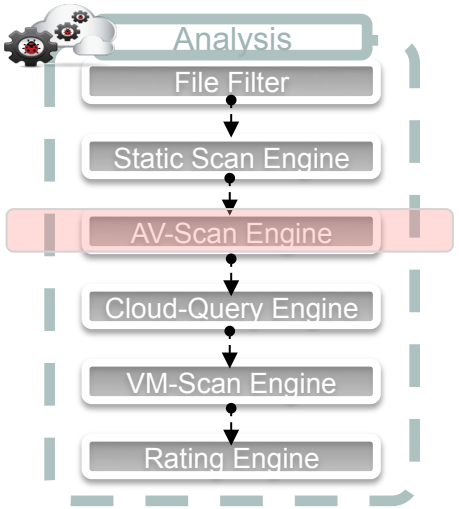
- Compact Pattern Recognition Language
- Used to write programs which detect virus behaviour
- Spots patterns in functionality and behavior (rather than just patterns of bytes)
- Performance: 1 complex signature catching 100,000 samples
- Resilience: Matching invariant patterns rather than whole files



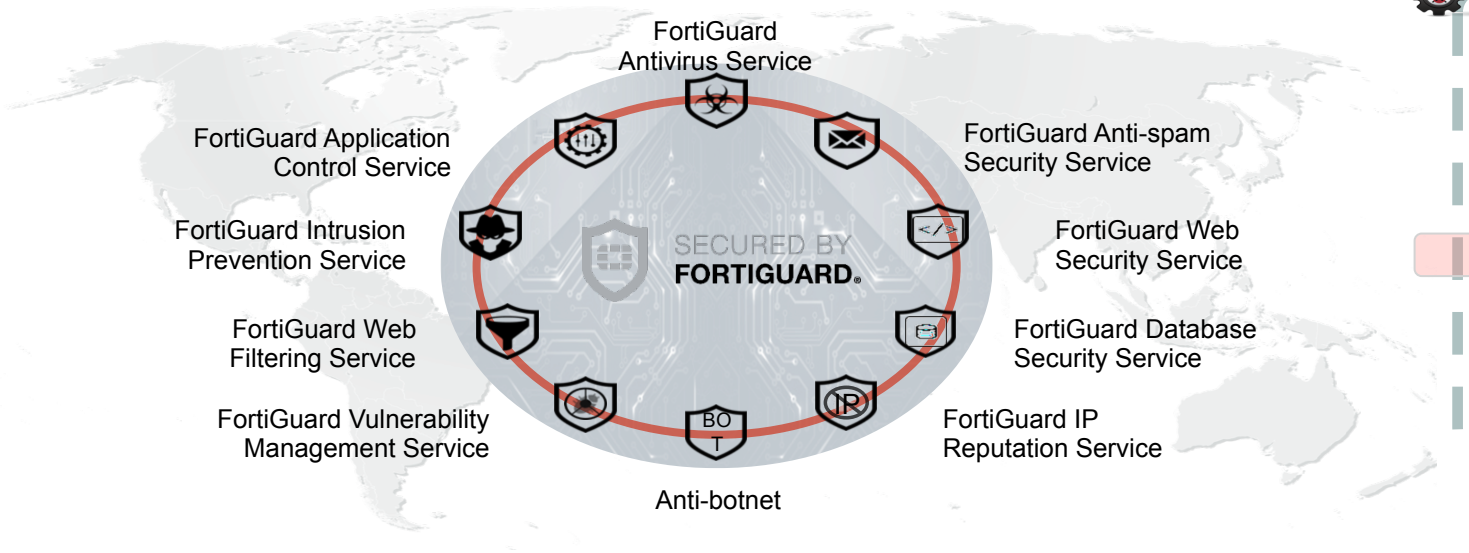
AV Scan Engine - Code Emulation

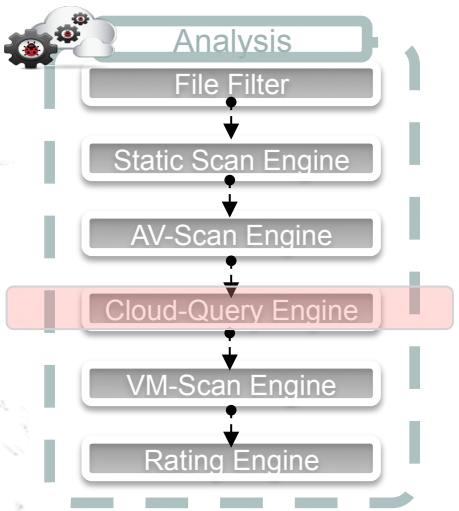
- Code emulation is the use of an emulator to review a program's code at a low-level without actually executing the code in question.
- Method can be utilized to determine program's goal or look for invalid or odd actions during normal execution.





FortiGuard Threat Research & Response





FortiGuard Minute

Per Minute

72,000
Spam emails intercepted

210,000
Network Intrusion Attempts resisted

68,000
Malware programs neutralized

310,000
Malicious Website accesses blocked

67,000
Botnet C&C attempts thwarted

34 Million
Website categorization requests

Updates Per Week

53 Million
New & updated spam rules

100
Intrusion prevention rules

920,000
New & updated AV definitions

1 Million
New URL ratings

8,000
Hours of threat research globally

SECURED BY
FORTIGUARD.

FortiGuard Database

150
Terabytes of threat samples

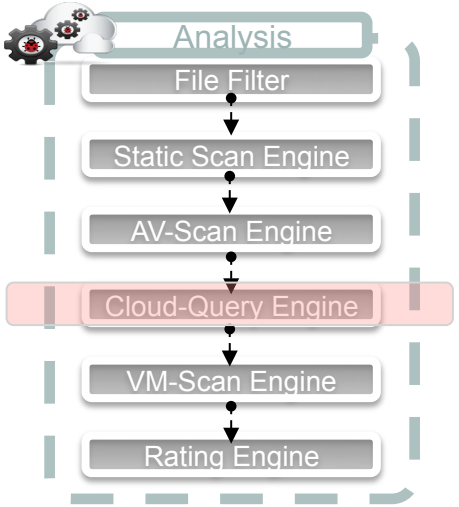
17,000
Intrusion Prevention rules

5,800
Application Control rules

250 Million
Rated websites in 78 categories

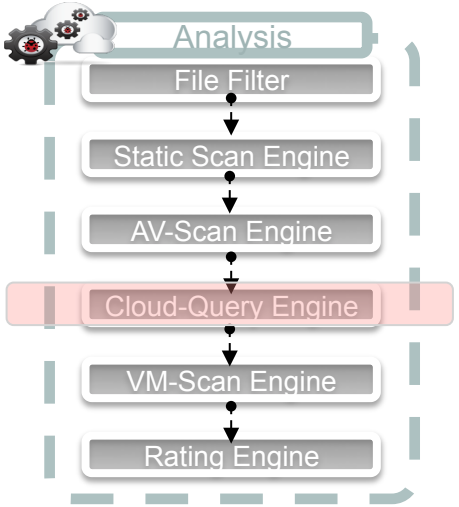
151
Zero-day threats discovered

Based on Q4 2014 data



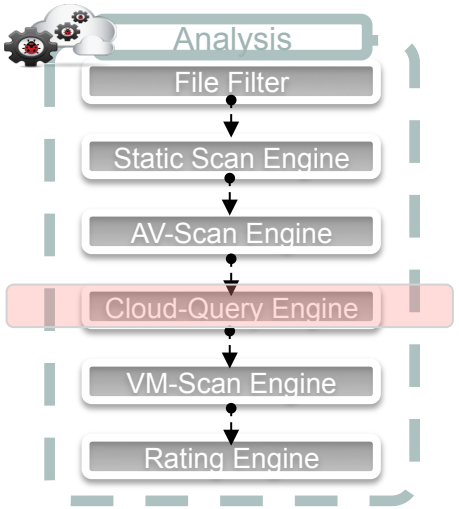
FortiGuard Services

- Cloud File Query
  - » Requests the FortiGuard Community
  - » Sends hash of samples
  - » Receives a verdict and a report of their analysis
- Cloud File Submission (on completion of processing suspicious file)
  - » Feeds the FortiGuard Community
  - » Shares the threat intelligence of a suspicious samples
  - » Sends the sample's content and the report of the analysis



FortiGuard Services (cont.)

- URL Rating
  - » Identifies URLs directed to malicious web sites
  - » Checks if they belong to the global category Security Risk
- IP Reputation
  - » Detects connection attempts to C2 servers



Time to Protect – 2 Levels

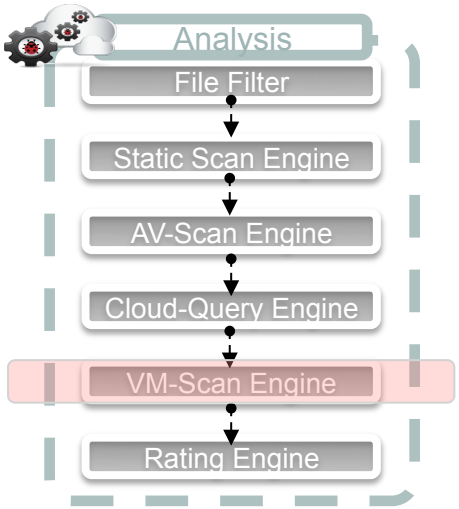
Time to Protect leverages two FortiGuard Services.

1. FortiSandbox Cloud Query
   - Every FortiSandbox can submit suspicious samples to FortiGuard
   - Every FortiSandbox can query FortiGuard about the latest suspicious samples
   - This availability of this information comes after an average of **3-10 minutes** after the initial suspicious sample submission

2. FortiGuard Signature Creation
   - If a submitted suspicious sample is confirmed to be malicious, a signature is created and installed into the next DB update
   - The new signature is available after a QA cycle which takes between **5-6 hours**
   - When the QA phase is complete, the DB update become available for every Fortinet product

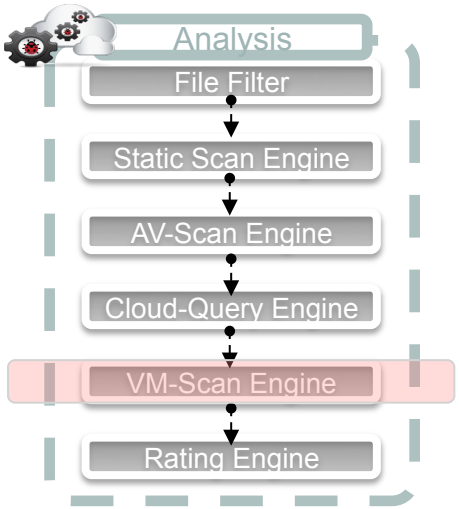
Virtual Machines

- Up until this point of the processing we support multiple Operating Systems
- Instantiate EXE/DLL, Office, JAR, SWF, exe components within archives (URL Detection) within a virtualized environment
- Supports files in **Windows XP, Win 7, Win 8.1, Win 10, Android** and **Custom Images**
- Collect behavior and network traffic to support rating
  - » Details of processes, registry changes, file system changes, network access are recorded for rating and reporting
  - » Provides snapshot for view if UI is used
- Rating in this environment will be seen as “Suspicious”



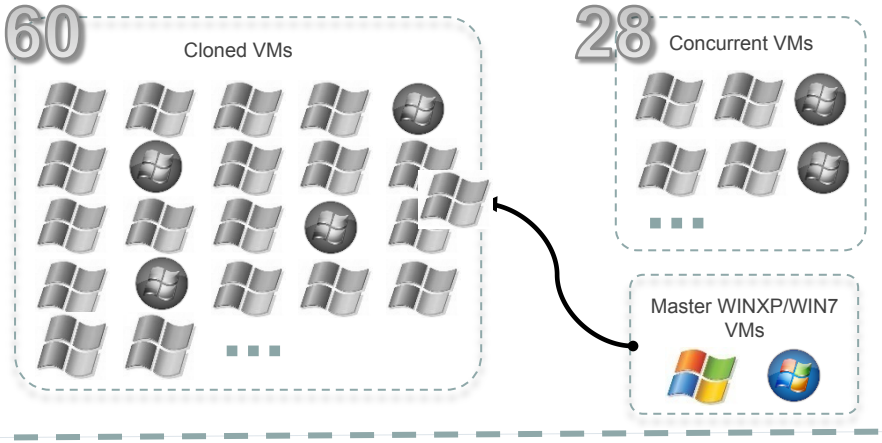
Virtual Machine Framework

- Flexible design that allows customisation
- Automatic VM package download (background)
- Automatic Windows License keys activation
- Efficient cloning process
  - » Adaptative clones number
  - » Stored in a memory file system
  - » Snapshot in a running state
  - » Revert to the initial snapshot after a sample execution

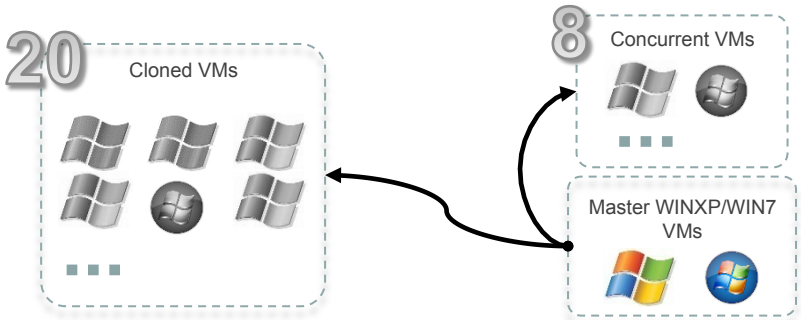


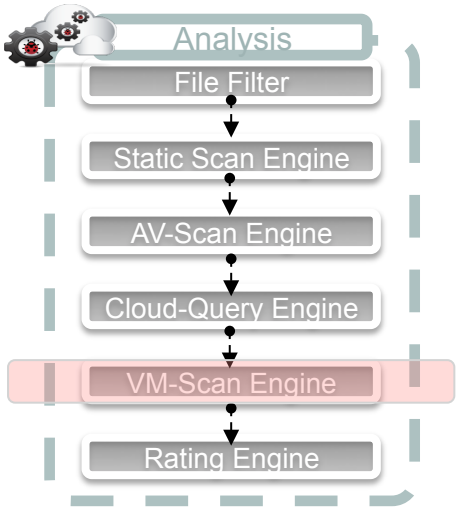
Virtual Machines Cloning

- FSA-3KD



- FSA-1KD

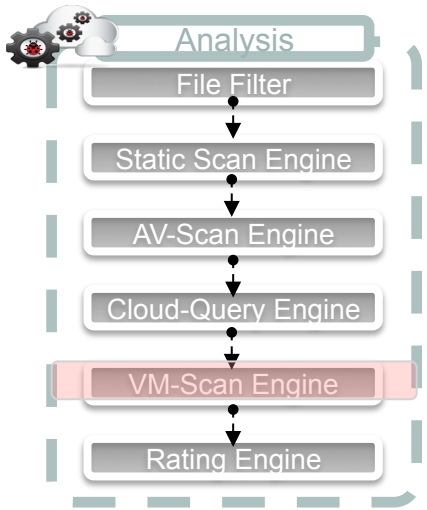




Virtual Machines

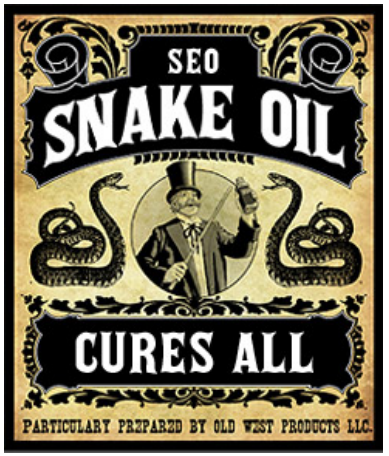
FSA-3KD	XP VM1	XP VM2	Win 7 x86	Win 7 / 8 / 10 x64
Totals	15	15	15	15
SWF	Internet Explorer 7	Internet Explorer 8	Internet Explorer 9	Internet Explorer 10
PDF	Adobe Reader 8	Adobe Reader 9	Adobe Reader 10	Adobe Reader 11
MS	MS Office 2007		MS Office 2013	

FSA-1KD	XP VM1	XP VM2	Win 7 x86	Win 7 / 8 / 10 x64
Totals	5	5	5	5
SWF	Internet Explorer 7	Internet Explorer 8	Internet Explorer 9	Internet Explorer 10
PDF	Adobe Reader 8	Adobe Reader 9	Adobe Reader 10	Adobe Reader 11
MS	MS Office 2007		MS Office 2013	
	Grand Total Capable:		8	



Custom VM Support

- FortiSandbox 2.2 Custom VMs
  - » Allows modification of existing FortiSandbox VMs
  - » Upload of custom Windows image
- Beware! custom image upload is not the elixir you believe it to be, please consider:
  - » Ongoing Support
  - » Advanced Evasion
  - » FSA Plug-In Support
  - » Threat Coverage (better with a ‘wide OS’)
  - » No additional file type coverage
  - » Updates

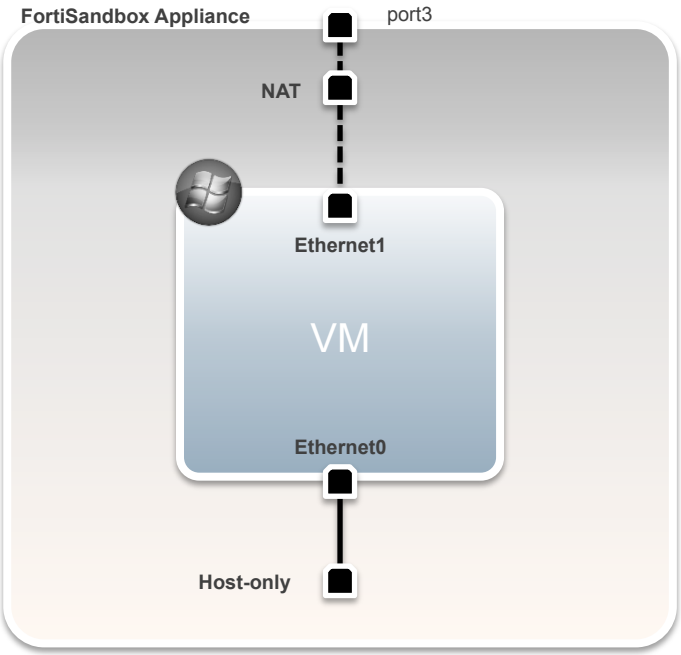


Tracer/Rating

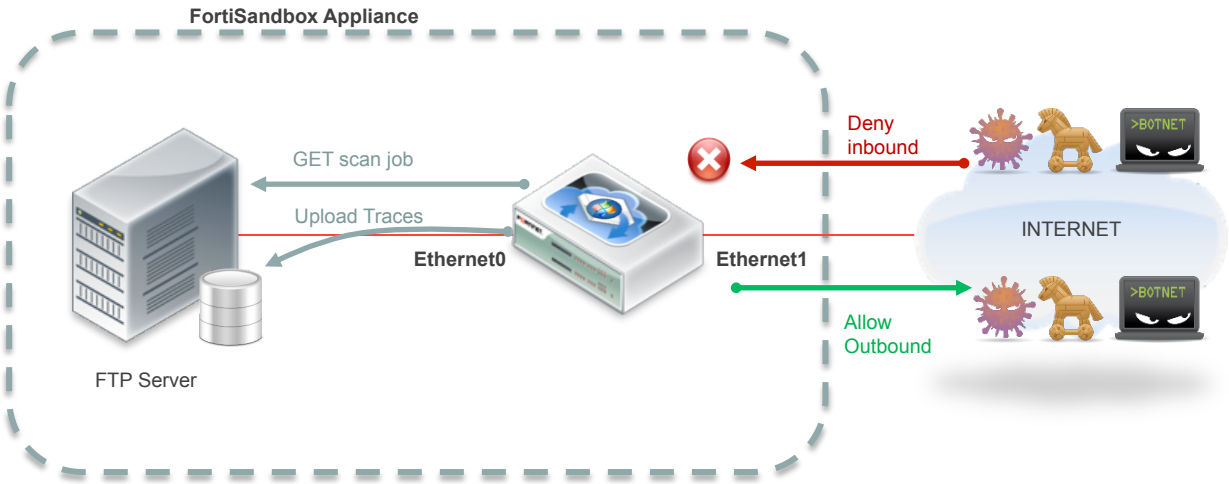
- Behavior of file is analyzed
  - » File System Behaviors
  - » Network Behaviors
  - » Registry Behaviors
  - » Memory Behaviors
  - » Over 55 behaviors rated
    - Persistence entries in registry
    - File creation (specific directories - %windir%)
    - Executable visits malicious site
- Network traffic also analyzed
  - » C&C IP address visited
  - » Launching of DDoS attack
- Negative Rating in this environment will be seen as “Suspicious”

Virtual Machine Network Design

Interface	Type	Network Setting
port3	Physical	Manually defined
NAT	Virtual network Adapter	192.168.57.2/24
Ethernet1	Bound to NAT	192.168.57.x/24
Ethernet0	Bound to Host-only	192.168.56.x/24
Host-only	Virtual network Adapter	192.168.56.1/24



Network Flow Paths of a Virtual Machine



Rating Engine

- Responsible for giving the final rating of a sample
- Uses the results of the different inspection features involved during its processing
- Calls some static engines to complete its inputs
- Analysis relies on the FortiGuard Labs' Threat Intelligence Knowledge
- Malicious, Suspicious High/Medium/low Risk, Clean

FortiSandbox Rating Definitions

- Malicious: 100% known malware
  - » Means that the detection comes from the local AV engine or
- Suspicious: malicious behavior detected but not 100% sure
  - » Severity helps to qualify the risk
  - » High: droppers, infectors, hijacker, etc.
  - » Medium: downloaders, worm, adware and greyware
  - » Low: riskware
- Clean/unknown: not detected as suspicious/malicious or cannot handle this file, or VM or Rating Engine timeout

FortiSandbox Sizing

FORTINET

Before You Start Sizing…..

- **Ensure you have answers for these questions:**
  - » Is the Sandbox part of an Inline Blocking solution or for Detection only
  - » Is the intention to block in ‘real-time’? (only possible with FortiMail and FortiClient)
  - » Is there a minimum response time for the Sandbox results?
  - » How will the files be submitted to the Sandbox?
  - » Which protocols will the files be extracted from? Any encryption?
  - » How many files per hour do you expect to be submitted to the Sandbox?
    - If unknown, will this be established during a PoC or is there something within the infrastructure that can help?

FortiSandbox Scaling

Supported File Type

New / Known Malware

Clean File

Or

Unknown Malware

pre-filters
15 - 20 seconds

up to
+ 2 ½ minutes

FortiSandbox

- File Filter
- Static Scan Engine
- AV-Scan Engine
- Cloud-Query Engine
- VM-Scan Engine
- Rating Engine

File Sizing Summary

- **This Means……(worse case scenario)**

Maximum of 3 minutes per file (60 minutes / 3) =
Maximum of 20 files an hour per Virtual Machine (if not caught by the pre-filters)

- **FortiSandbox Platforms**

- FortiSandbox-1000D (8 concurrent VMs * 20) = 160 files per hour
- FortiSandbox-3000D (28 concurrent VMs * 20) = 560 files per hour
- FortiSandbox-Base-Virtual Appliance (4 VMs * 20) = 80 files per hour
- FortiSandbox-Maximum-Virtual Appliance (52 VMs * 20) = 1,040 files per hour

- **Clustering Allows Up to 100 Members**

- In any platform combination (Initial Master / Primary Backup have to be the same)
- All cluster platforms share the file load / distribution
- Master loses 1 VM for every 5 VMs in the cluster

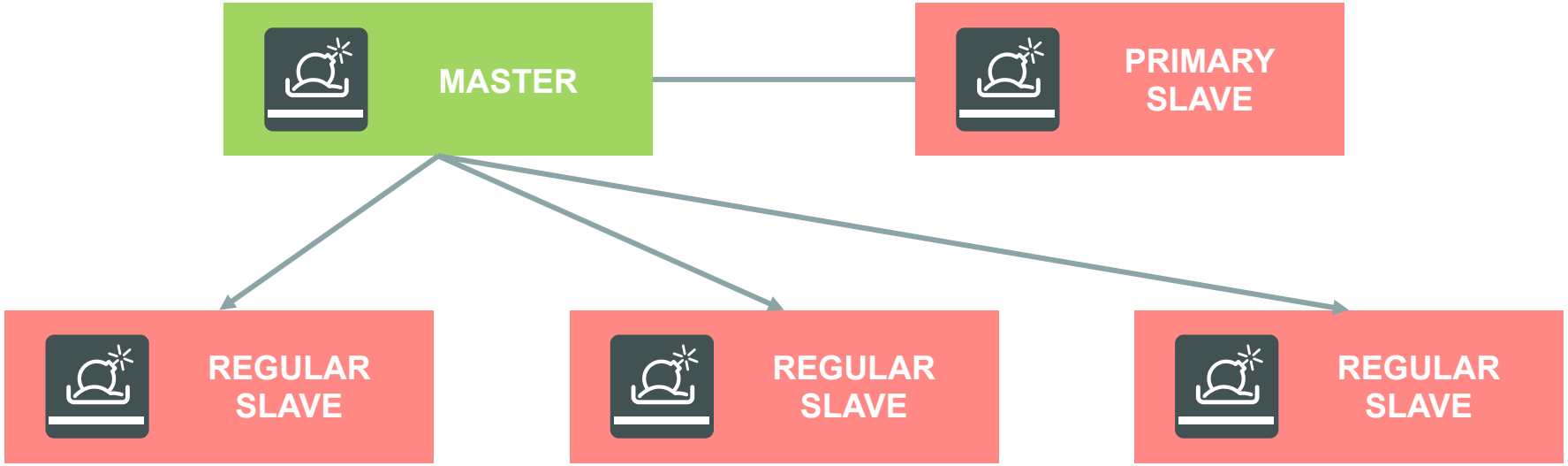
theoretical maximum 1,040 * 99 = 102,960 files per hour / 1,716 files per minute / 28.6 files per second

Clustering

FORTINET

Clustering and Load Balancing

- Master and Primary Slave have to the same appliance (can be any model)
- Regular Slaves can be any appliance
- Up to 100 nodes in a cluster



Clustering – The Sacrifice of the Master

- As soon as a FSA cluster is formed the Master operates 50% of its VM capacity and the Primary Slave operates 100% of its VM capacity
- Master is responsible for job distribution and cluster management so it needs to dedicate processing power to these tasks
- Recommendation is that for every 5 VMs on the slaves, 1 VM should be removed from the Master

Clustering – The Sacrifice of the Master…continued

- For example, x2 FSA3KD Cluster on default settings
  - » FSA3KD Master operates 14 VMs (half the normal amount)
  - » FSA3KD Primary Slave operates 28 VMs
    - 28 slave VMs / 5 = 6
    - So Master should be running 22 (28 – 6) VMs, but its running 14 by default
    - The CLI command '`hc-master -s75`' takes the Master back to 75% of its VM processing power which is 21
    - 49 VMs available in Cluster, worse case file processing scenario is (3 minutes per file, 20 files an hour, 20 * 49) 980 files per hour

Dynamic Malware and URL Packages

FORTINET

Malware Package

- Dynamic Signature list exclusive to FortiSandbox
  - » Any sample rated Malicious (known existing signature), High or Medium Risk (no known signature) can be added to the Malware Package
  - » FortiGate's and FortiClient's registered to FortiSandbox, pull down the Malware Packages periodically
  - » FortiMail checks the file hash against the FortiSandbox DB before submitting the file to FortiSandbox (so need for local copy)
  - » Malware Package contents available at *File-Based Detection>File Input>Device*
  - » Malware Packages contents optionally uploaded to FortiGuard, so that a signature can be created

URL Package

- If a sample is downloaded from a URL, and the sample is Malicious or Suspicious, then the URL is added to a Dynamic URL list

High Risk Dropper

Mark as clean (false positive)

Sample Report

Received	Jan 25 2016 08:37:21
Started	Jan 25 2016 08:37:24
Status	Done
Rated By	VM Engine
Submit Type	FortiGate
Source IP	10.1.1.105
Destination IP	192.168.152.194
Digital Signature	No
Scan Bypass Configuration	N/A

	Rating
lwareserver.com/dangerous_dropper.exe	High Risk
server/veil27.exe	Malicious
server/fsa_dropper.exe.00000000000000000011.incr.exe	High Risk

File-based Detection>File Input>Device>URL Packages>URL Package Version

More Details

Behavior Summary

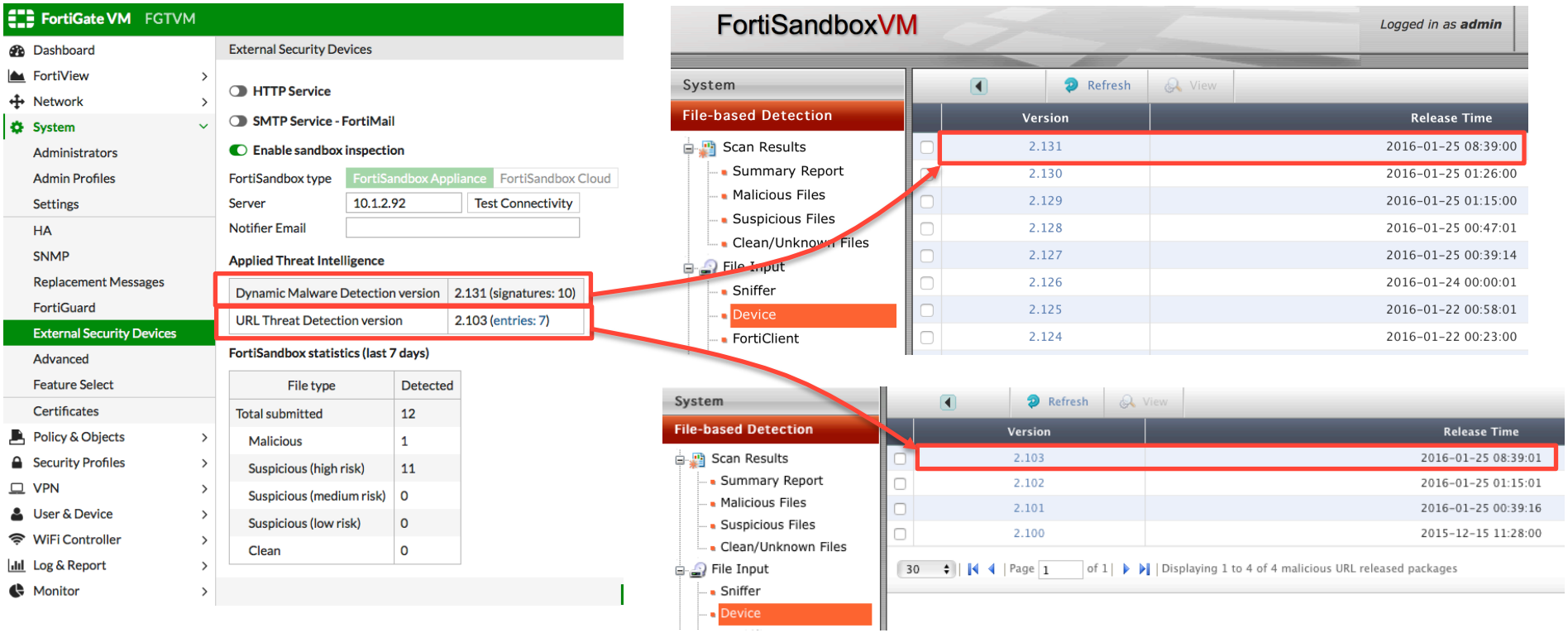
This file dropped files

Analysis Details

Packer	N/A
File Type	exe
Downloaded From	http://www.malwareserver.com/dangerous_dropper.exe

- Download URL discovered during sample analysis
- URL added to FortiSandbox URL Package and pushed down to Fortinet Devices

Malware and URL Packages on FortiGate



FortiMail and FortiSandbox

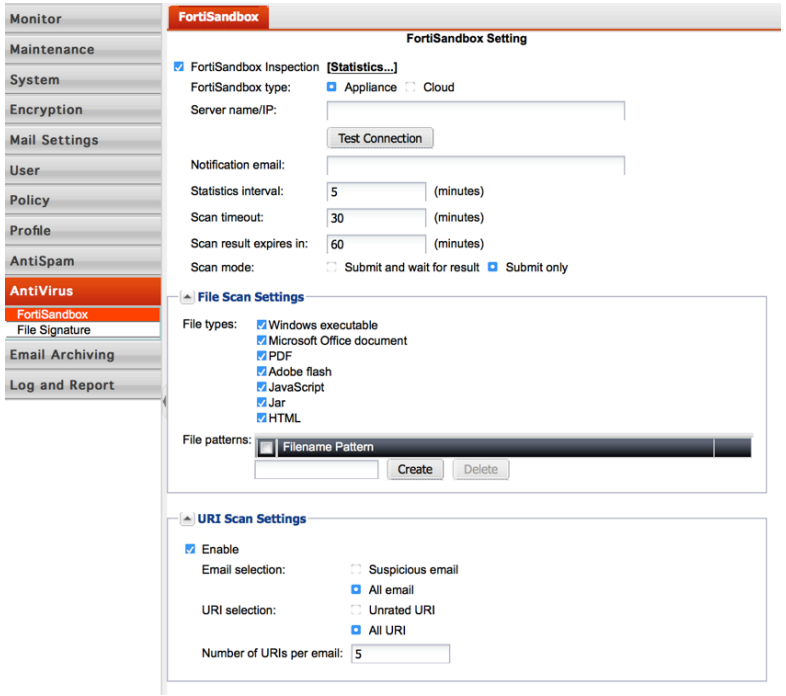
FORTINET

FortiMail and FortiSandbox Integration

- One of the strongest components of the ATP Framework
- According to Verizon's 2014 Data Breach report, 80% of Enterprise malware still comes in via mail
- Verizon's 2015 Data Breach report stated that 50% of phishing links sent via mail are clicked on within an hour of them reaching the inbox
- Block Inline and in Real-Time

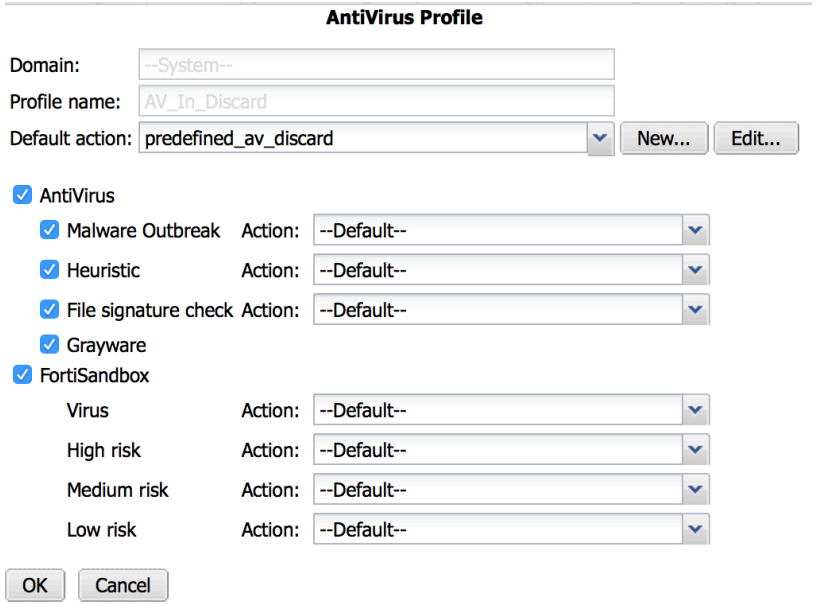
FortiMail – Controlled File Submission

- Selective File Submission and URL Submission

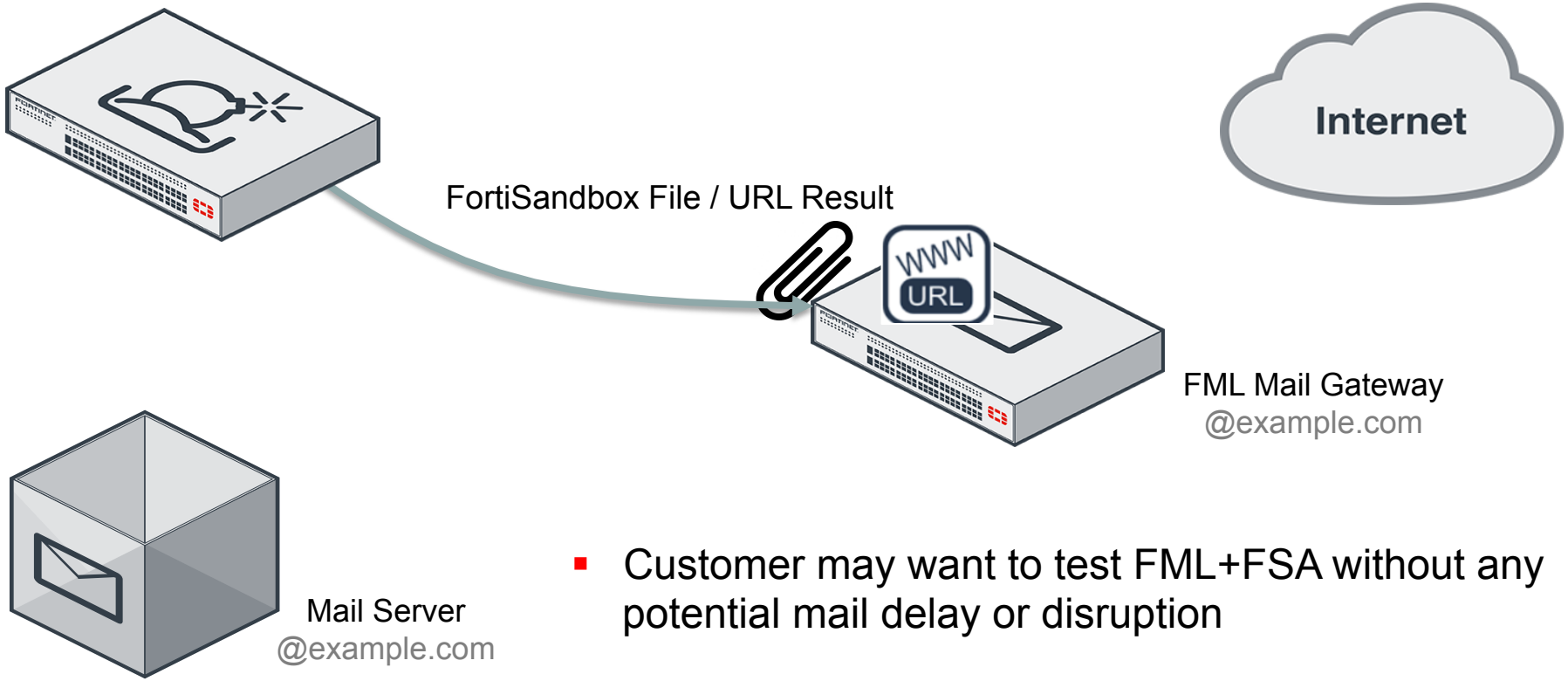


FortiMail – Selective Action

- Configurable Actions based on FortiSandbox Result
  - » Pre 5.3, all Malicious ratings were hard coded to be dropped

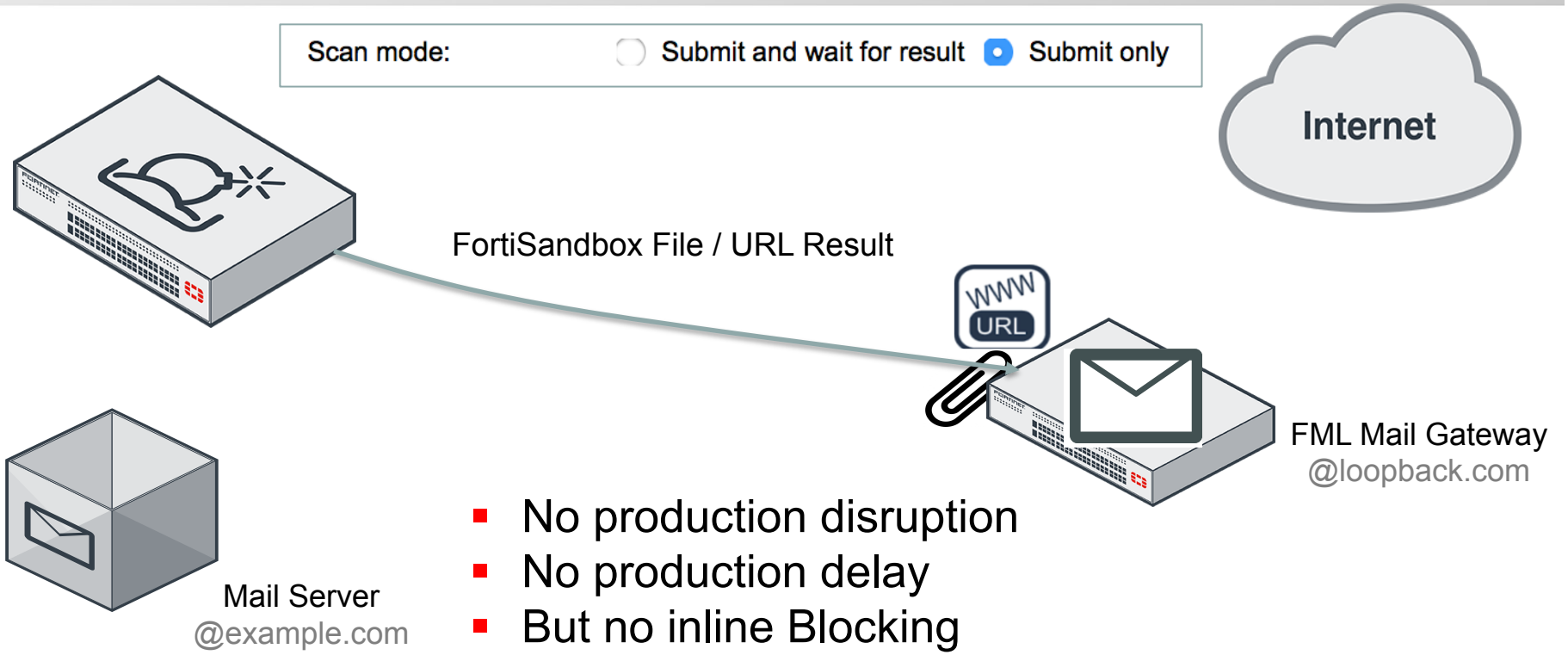


FortiSandbox and FortiMail Typical Inline Deployment



- Customer may want to test FML+FSA without any potential mail delay or disruption

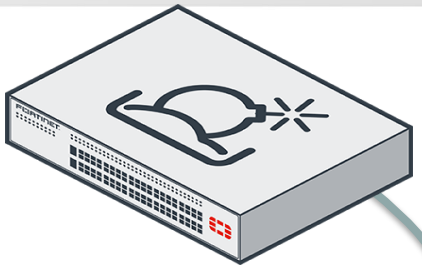
FortiSandbox and FortiMail – 'Submit Only'



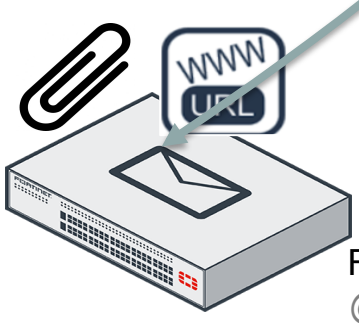
- No production disruption
- No production delay
- But no inline Blocking

FortiSandbox and FortiMail – 'Always BCC'

- Mail Gateway has to support all-bcc
- Once off-path Mail Server mailbox is full, it won't accept anymore mails
- No disruption or delay, but no inline Blocking

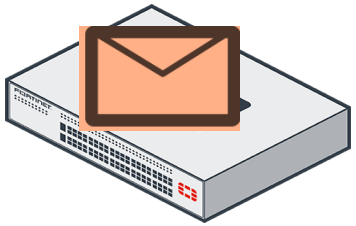


FortiSandbox File / URL Result

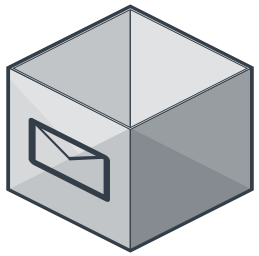


FML Mail Server
@loopback.com

bcc
fsa@loopback.com

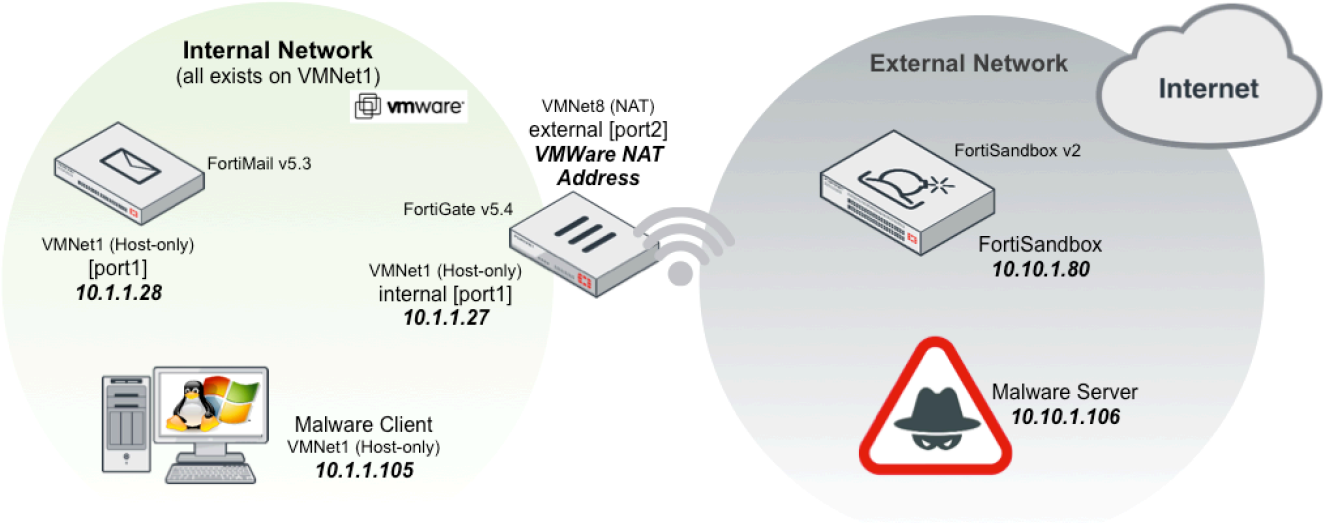


FML Mail Gateway
@example.com



Mail Server
@example.com

Lab Topology



SSID: APT-WKSHP
Key: f0rtinet@123
IP Range: ***10.10.1.110-210***

Whatever the VMWare NAT Address will be (can be anything but typically on a 192.168.x.x range), it will bind and NAT to the Laptop Address ***10.10.1.__***

Username/Password
FortiGate: admin / *blank*
FortiMail: admin / *blank*
FortiMail User: test / *fortinet*
Malware Client: malware-client/ *fortinet*
FortiSandbox: admin / *fortinet*

Lab Time

If you're VMs and lab environment are not pre-prepared then

You're **O**n **Y**our **O**wn

Lab 1

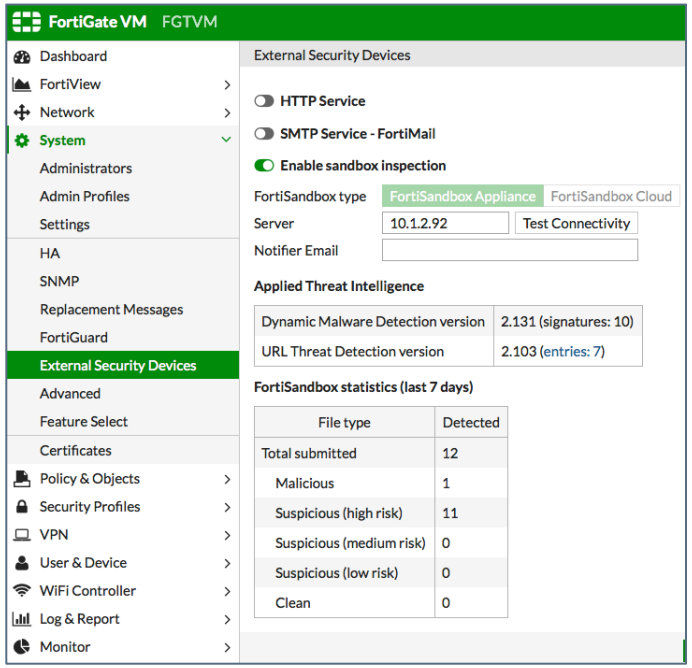
FortiMail and FortiSandbox

FortiGate and FortiSandbox

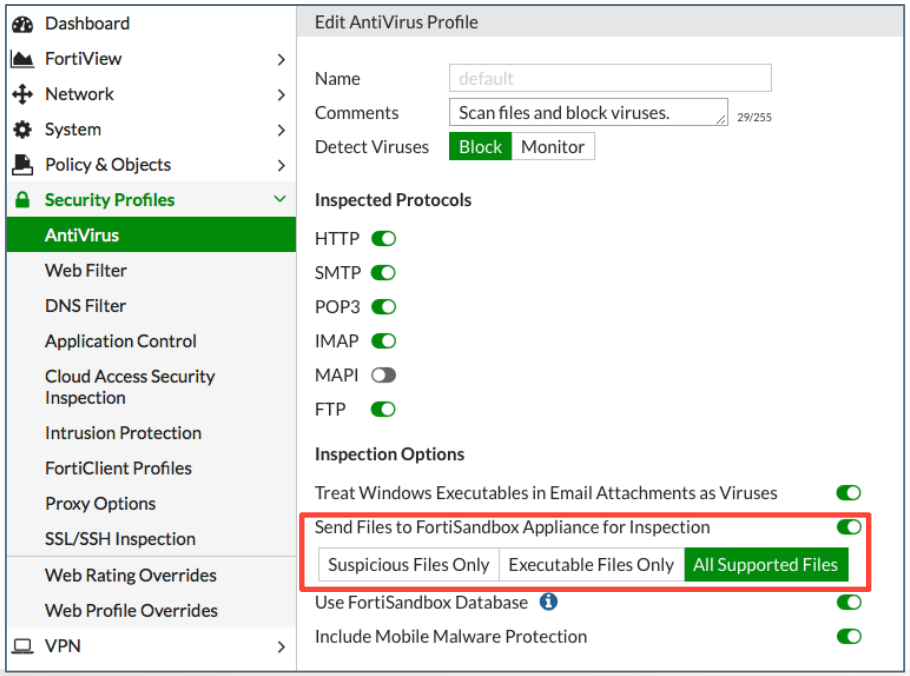
FORTINET

FortiGate and FortiSandbox

- Appliance or Cloud Sandbox enabled under System settings



- Applied on the AV profile and used in Policies



Threat Mitigation

Prevent Others From Infection

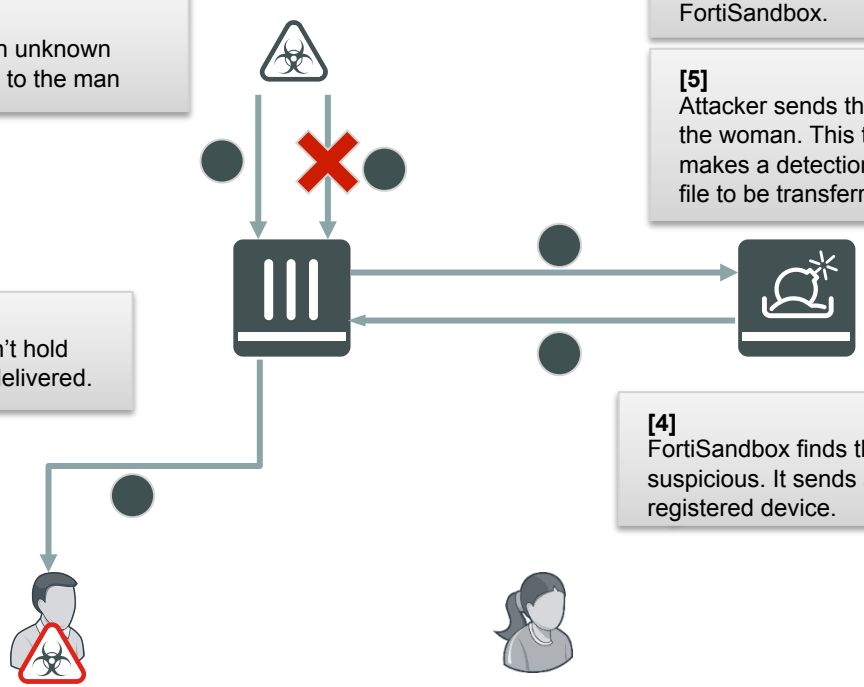
[1]
Attacker sends an unknown malicious sample to the man

[2]
FortiOS performs AV inspection but as it is unknown it submits it to FortiSandbox.

[3]
As FortiOS doesn't hold the sample, it is delivered.

[4]
FortiSandbox finds that the sample is suspicious. It sends a DB update to the registered device.

[5]
Attacker sends the same sample to the woman. This time AV inspection makes a detection and prevents the file to be transferred.



Lab 2

FortiGate and FortiSandbox

FortiClient and FortiSandbox

FORTINET

Fortinet's FortiClient Endpoint Protection Platform

Unified Client

- Antivirus
- Web Filter
- Application Firewall
- Vulnerability Scanning
- 2-Factor Authentication
- Remote VPN
- WAN Optimization
- Part of Fortinet's ATP System (Sandbox Integration)

- ✓ Top rated protection
- ✓ Easy deployment
- ✓ Low TCO

Independent Validation

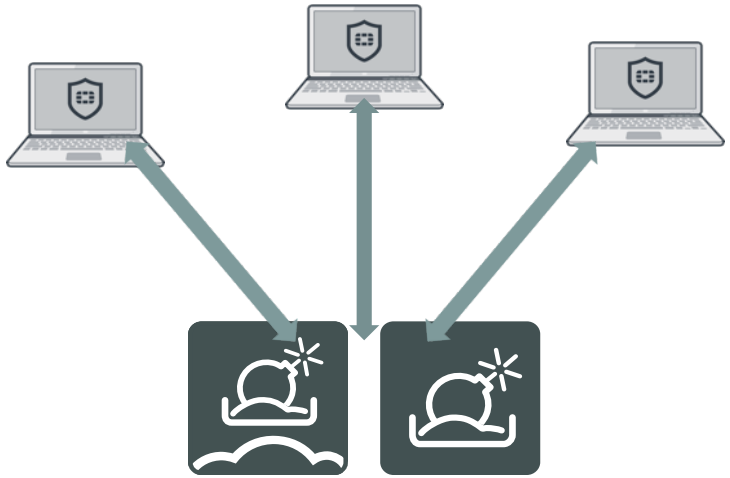
NSS LABS RECOMMENDED

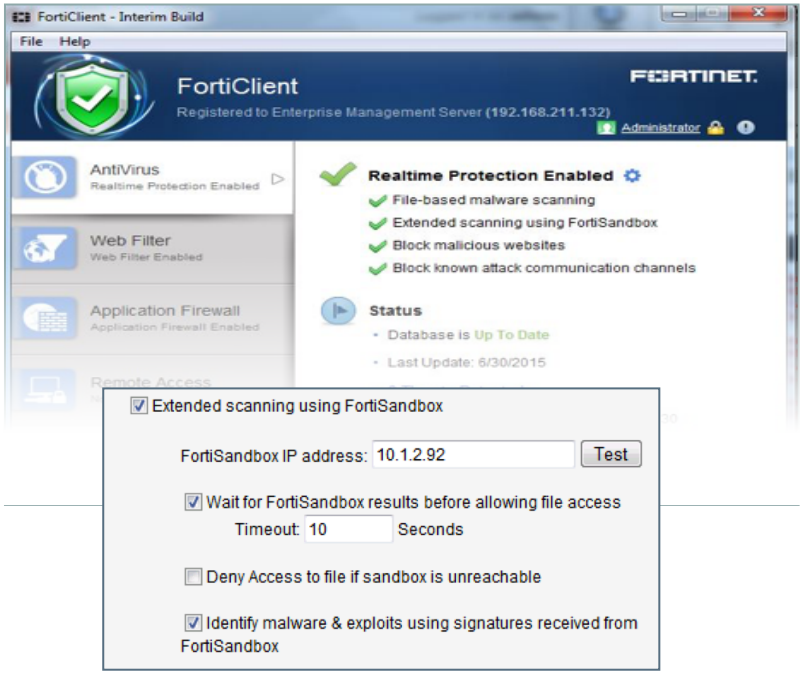
vb 100 VIRUS virusbtn.com

AV comparatives ADVANCED+ ★★★ -REAL WORLD- PROTECTION TEST JUL 2015

FortiClient Integration

- Hold For or Act Upon Result
- Dynamic, Local Threat Intelligence



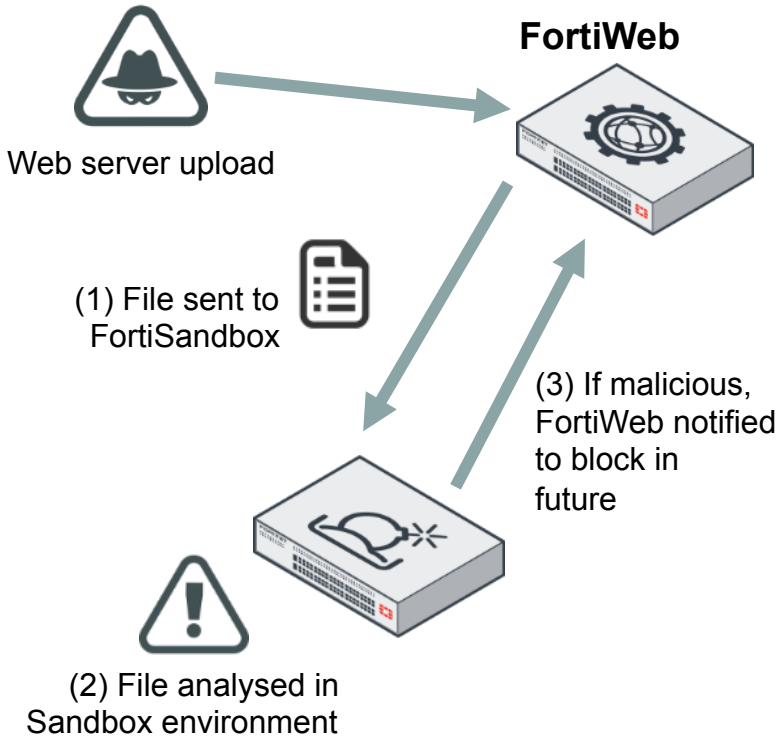


FortiWeb and FortiSandbox

FORTINET

FortiWeb Integration

- Direct integration for advanced threat detection
- Web application file uploads cleared by FortiWeb's AV scanner are sent to FortiSandbox for analysis
- FortiWeb notified if threat detected
- If determined to be a threat, FortiWeb blocks all future instances



Lab 3

FortiClient, FortiWeb and FortiSandbox Demo’s

Additional Considerations

FORTINET

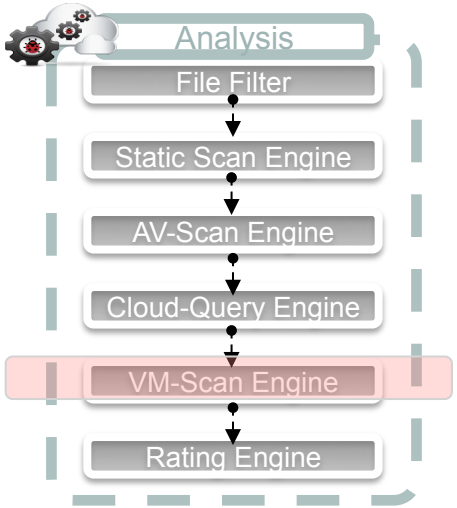
Advanced Evasion Techniques

The CPRL engine is able to detect:

- Logic Bombs
- Rootkits & Bootkits
- Sandbox detection
- Botnet C2 Window
- Network Fast Flux
- Encrypted Archives & Binary Packers
- Polymorphic Malware

Web Sites Scanning

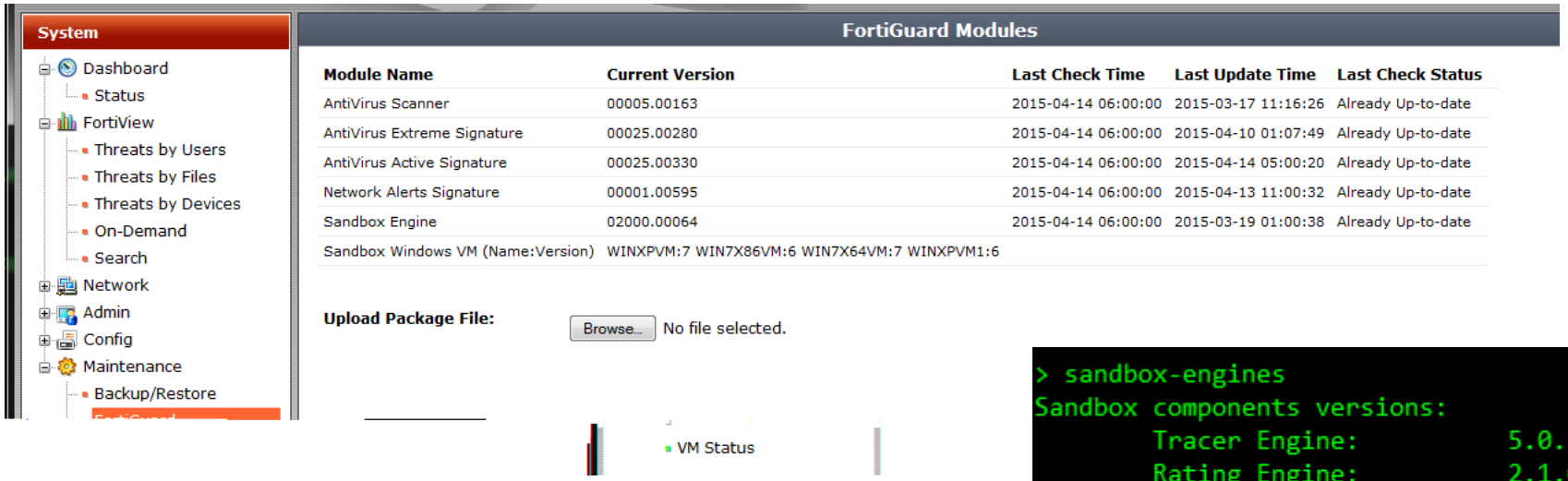
On-demand URL inspection



- Inspects URLs submitted through a file of URLs
- Dedicated section in the GUI: URL Detection
- Scan Profile
  - » Select IE versions to use
  - » Control the URLs number in the list
- Depth and Timeout configurable in the On-Demand submission form
- Updated JSONRPC-API

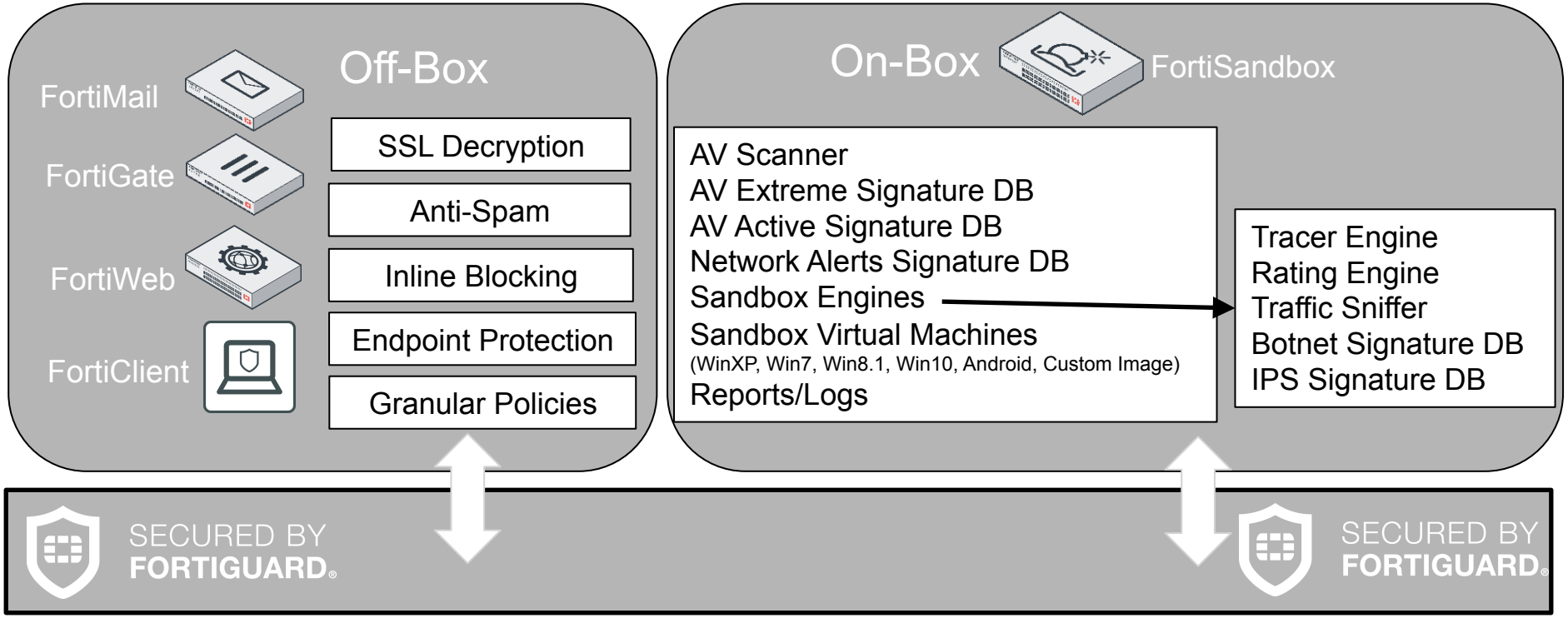
On-Box/Off-Box Modules

- Available on FortiSandbox



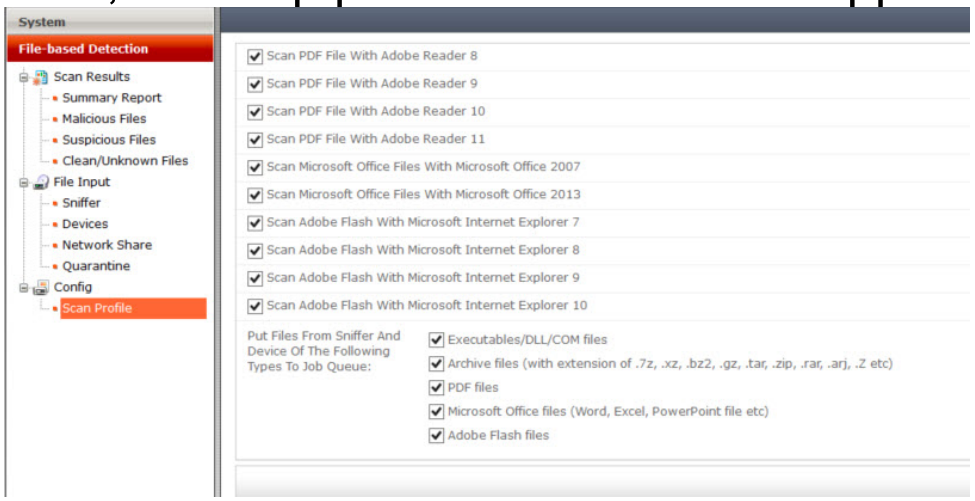

```
> sandbox-engines
Sandbox components versions:
        Tracer Engine:          5.0.545
        Rating Engine:          2.1.054
        Traffic Sniffer:        3.0.071
        Botnet Signature DB:    2.189
        IPS Signature DB:       5.631
```

On-Box/Off-Box Features



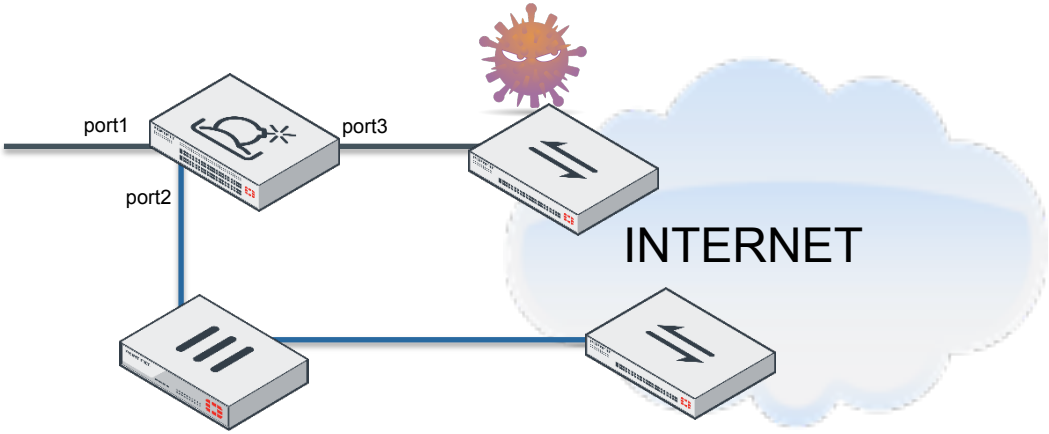
FortiSandbox Granular Scan Profiles

- New ability to eliminate files from review if required
- Resource management provisioning in the new version
  - » Can cause FSA to drop certain file types even before AV scan
  - » Can allow AV scan, but drop prior to VM based on application



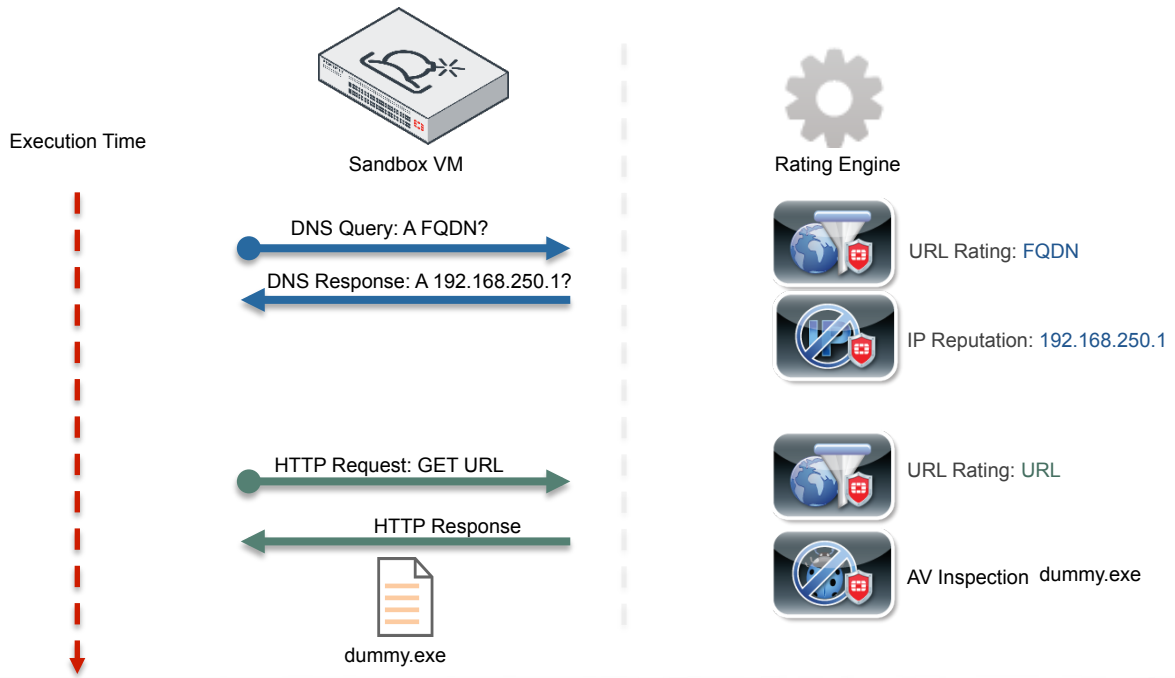
SimNet – Open or Closed Environment

- Should you risk to degrade your IP reputation by allowing sandbox VM going through your Internet access?
  - » Sandbox VM execution is short
  - » Your reputation is at risk every day (i.e. infected computer in your network)
  - » Use a dedicated Internet access for FortiSandbox outgoing traffic



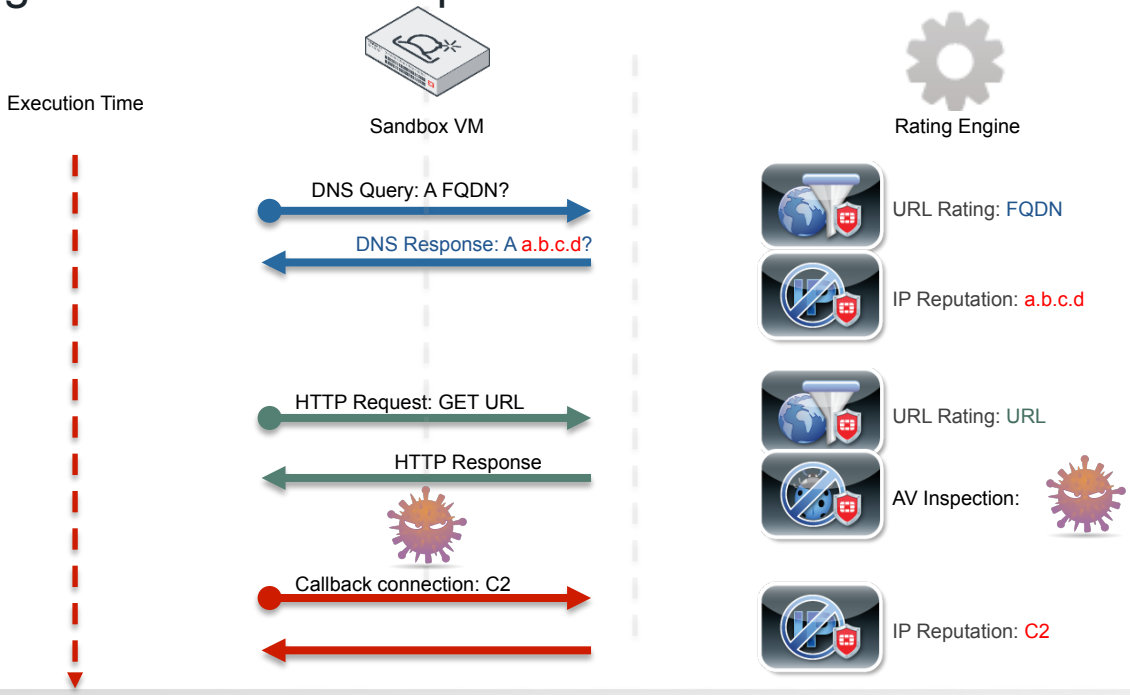
Why Internet Access is Important for Detection

- Detonating a downloader sample into a sandbox VM with the *netsim* feature enabled



Why Internet Access is Important for Detection

- Detonating a downloader sample into a sandbox VM without *netsim*



Network Proxy Support

- Alternative to *SimNet* using the corporate proxy server
- Network Proxy Service
  - » Sandbox VM
  - » FortiGuard Services
- Supported Protocols
  - » HTTP CONNECT
  - » HTTP RELAY
  - » SOCKS v4/v5
- Constraints:
  - » Must use an DNS server that forwards lookup for external RRs
  - » Proxy must be reachable through interface port3

Rescan

	Filename	Rating
	veil3.exe	Malicious

Originally scanned as clean

Rescan then found it to be a recognised virus

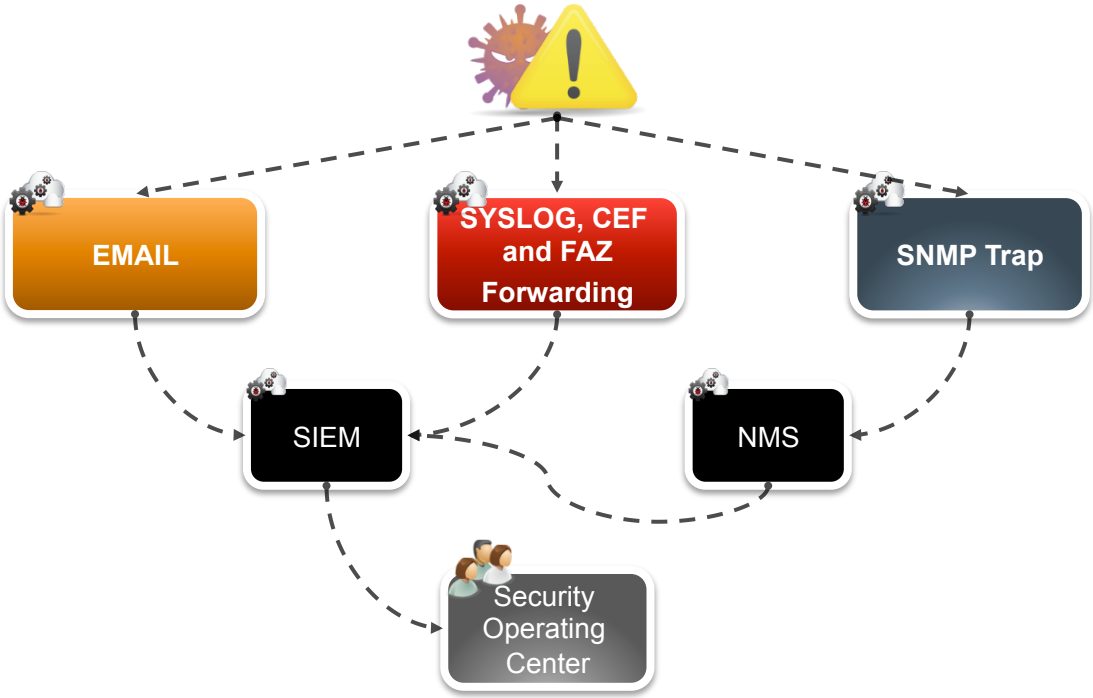
- Rescan carried out on every AV update
- Last 48 hours worth of clean files are rescanned

Output Options

FORTINET

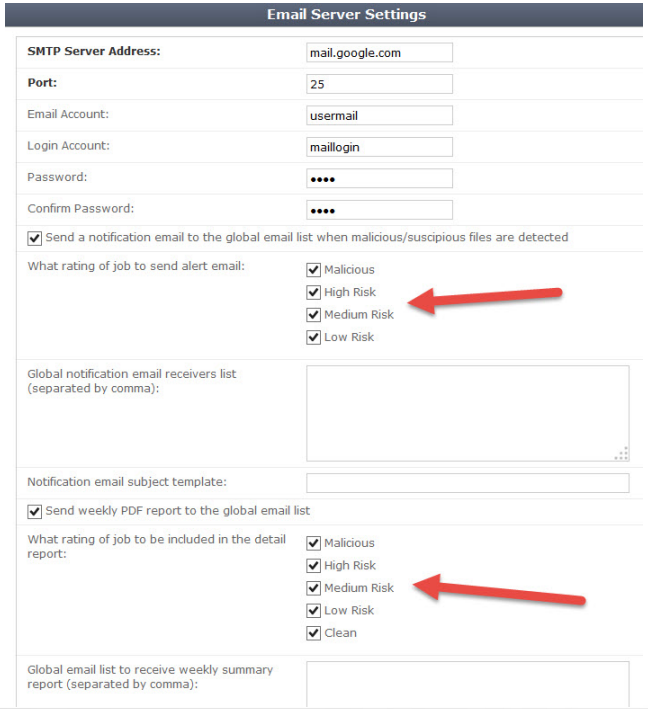
Notifications

- Notifications and alerts sent for malicious and suspicious findings



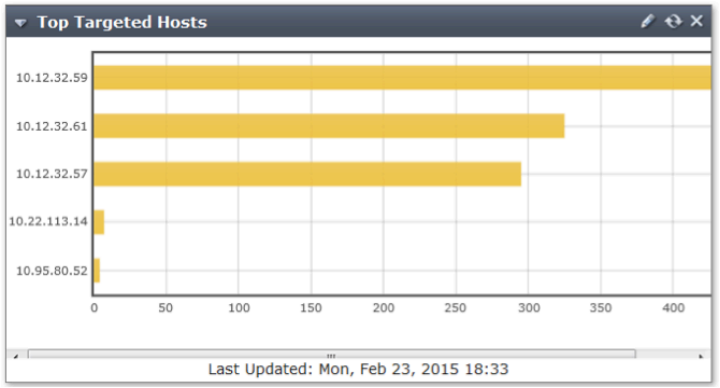
Email Notification and Reporting Granularity

- Email alerting remains but granular control for notifications and reporting.



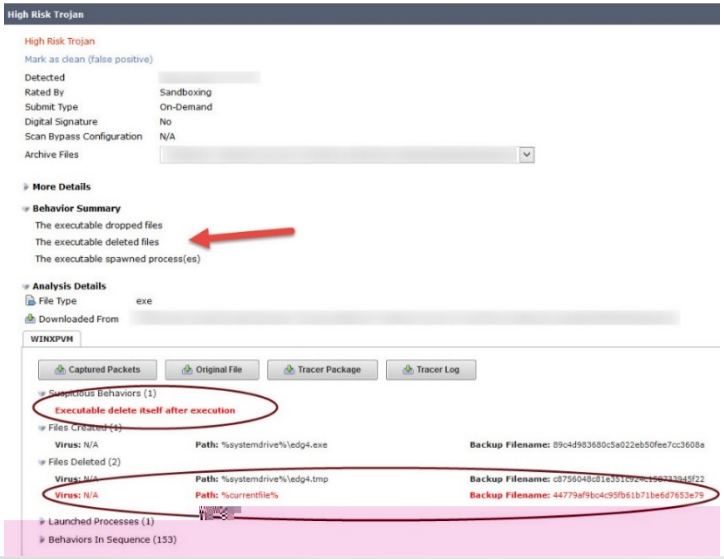
Scan Views

- Maintains summary views
- Overall capability to see scan job from Suspicious File screen
- Provides capability to dig into file to extreme granular level



Scan Results

- New Detail Layout calls out particulars
  - » Even within the detail of the output
- Notice red callouts in behaviors



Scan Results

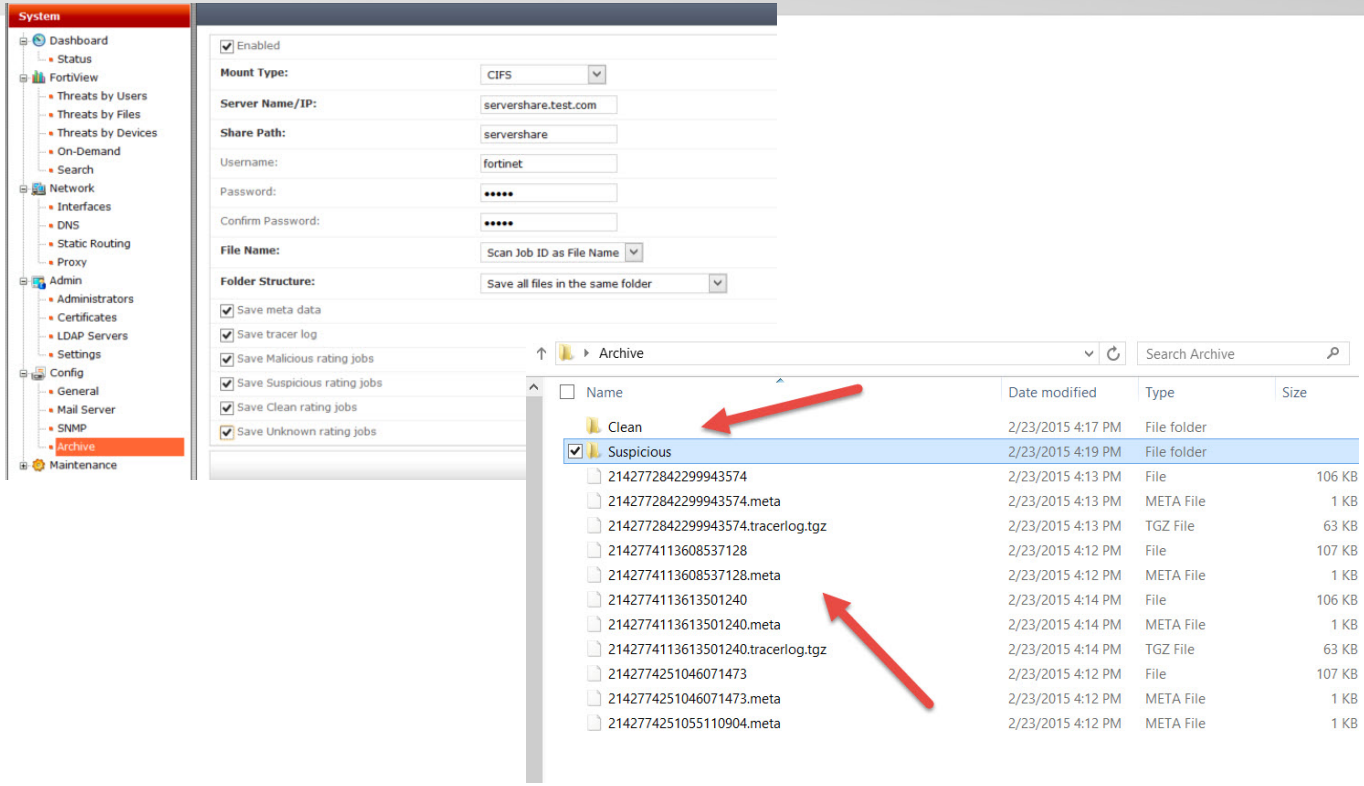
- That detail continues even throughout sequence of behaviors
- Enables Administrator to quickly see dangerous behaviors through every behavior that was documented

Time: 15:11:26	**Type:** Registry	**Operation:** Set value	**Detail:** Key:HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\EventMessageFile;Data:%SYSTEMROOT%\system32 \ESENT.dll;DataType:2	
Time: 15:11:26	**Type:** Registry	**Operation:** Set value	**Detail:** Key:HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\CategoryMessageFile;Data:%SYSTEMROOT%\system32 \ESENT.dll;DataType:2	
Time: 15:11:26	**Type:** Registry	**Operation:** Set value	**Detail:** Key:HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\CategoryCount;Data:16;DataType:4	
Time: 15:11:26	**Type:** Registry	**Operation:** Set value	**Detail:** Key:HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\TypesSupported;Data:7;DataType:4	
Time: 15:11:26	**Type:** File system	**Operation:** Delete file	**Detail:** FilePath:%CURRENTFILE%;Size:108544;MD5:01F2A64AA594FCEAB838F8818A312A44;FileType:EXE;bak:backup\44779af9bc4c95fb61b71be6d 7653e79	Executable delete itself after execution
Time: 15:11:27	**Type:** Registry	**Operation:** Set value	**Detail:** Key:HKLM\SOFTWARE\Microsoft\Cryptography \RNG\Seed;Data:4EBF76ACE6039AF8ECD7B6D7DD25F549E27A7AF505C6130928F122B9ACDB2646964C90C8496D280C080A3DFA463F14EE3F D7E4E5AB7DBD938DDD06A050C43748171D6654CD5FA488AEF8B231517D8287;DataType:3	
Time: 15:11:27	**Type:** Registry	**Operation:** Set value	**Detail:** Key:HKLM\SOFTWARE\Microsoft\Cryptography \RNG\Seed;Data:7215977026A30404F19F33548BD59C30EB576754319240 0SD70D2BA8AF2A55FE761A5D62CD9EF26D74CC9DAD665DF7330 8EB2E0FF5DDB92EDA73803CC3526FA5796A760F27FA6AB9FEE053A9F3E0AB1;DataType:3	
Time: 15:11:27	**Type:** Registry	**Operation:** Set value	**Detail:** Key:HKLM\SOFTWARE\Microsoft\Cryptography	

Archival Capability

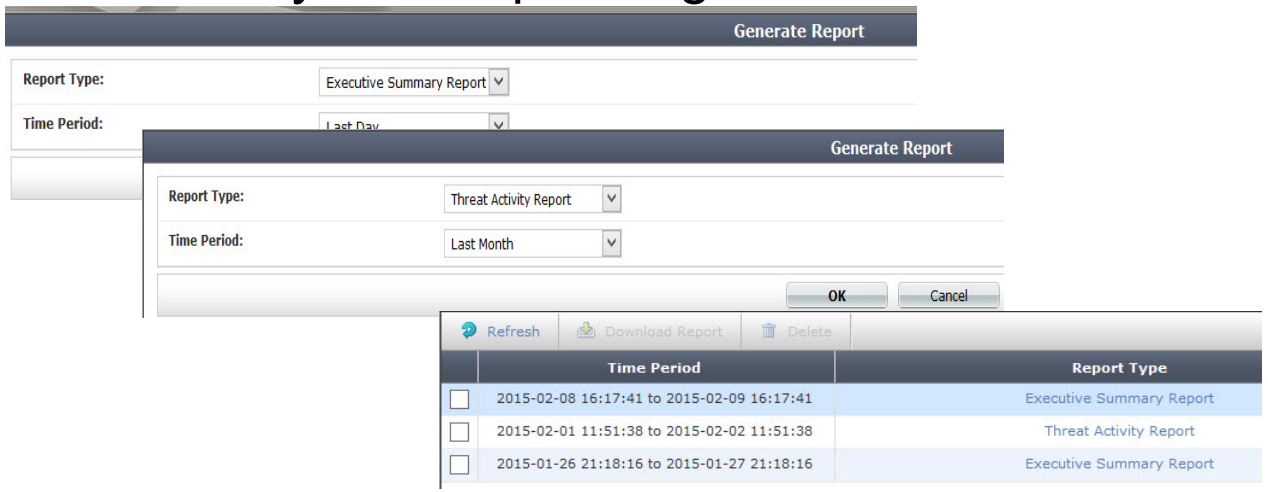
- Provides capability to off-load storage and maintain
- Provides location for secondary scanning of a 3rd Party Tool
- Archive support is per FSA
- Granular control for storage
  - » meta data, Tracer log
  - » Per rating (or all) Malicious, Suspicious, Clean, Unknown
- Structure of maintained information is configurable
  - » Store by file name or job ID
  - » Save all files in one folder
  - » Save file in folders based on scan finish time
  - » Save file in folders based on ratings

Archival Capability



Report Capabilities

- Reporting options are now able to be generated
  - » Different reports
  - » Different time periods
- Access immediately after report is generated



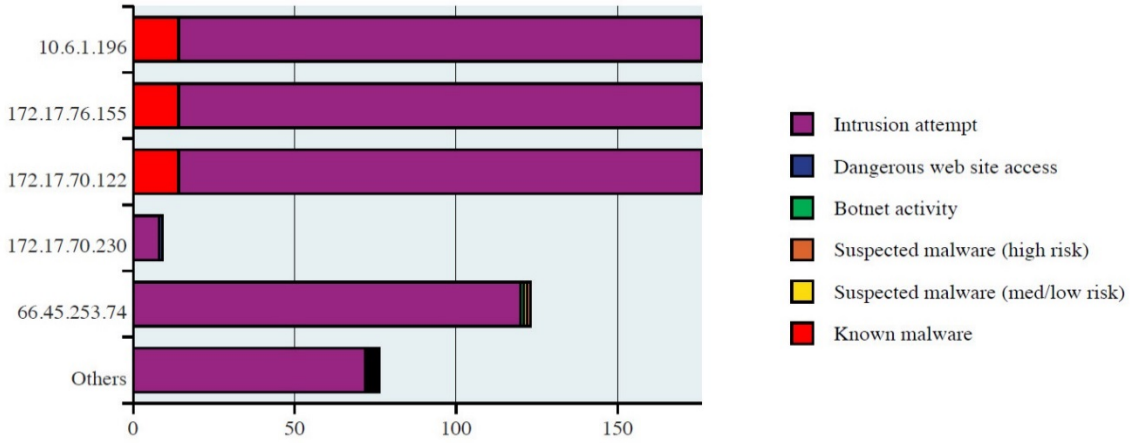
Automated Report Views

FortiSandbox Executive Summary Report

Automated Report Views

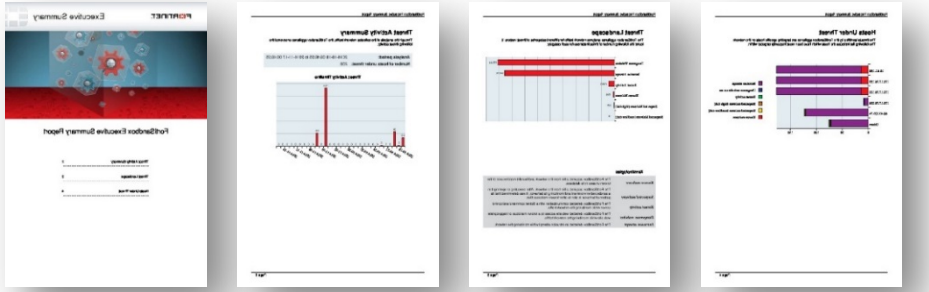
Hosts Under Threat

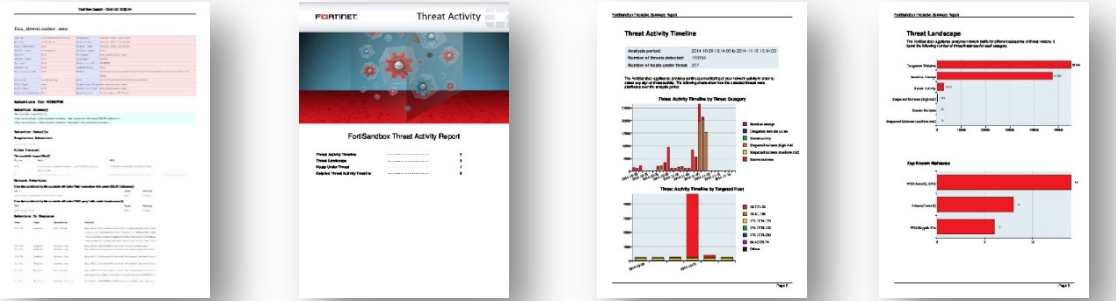
The threats identified by the FortiSandbox appliance are targeting specific hosts on the network.
The following list indicates the hosts which have been most frequently targeted within.



Reporting

- Executive Summary Report
- Threat Activity Report
- Detailed Report





Lab 4

API and FortiSandbox

Lab 5

Malware Demos

FORTINET®